SoCal Privacy Consultants

*Operationalizing Privacy and Security Programs*

# New Cybersecurity, Cyber Insurance & Privacy Risks

## *Knowledge is Power*

## *What You Need to Know to Mitigate These Risks*

**FENG Monthly Meeting**

Tuesday, February 4, 2020 | 8-10am
PricewaterhouseCoopers (PwC) Office
5375 Mira Sorrento Place, Ste 300 (3rd flr), San Diego, CA 92121

**Michael H. Cox, CIPP/US**
CEO and Founder
Chief Privacy Consultant
**Neil R. Packard, CISA & CIPM**
Chief Security Consultant

# BIOs of Principals

## Michael H. Cox, CIPP/US

- ❑ CEO/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, CIPM

- ❑ 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)
- ❑ Certified Information Privacy Management (CIPM)
- ❑ 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

# Today's Objectives

- ❑ Understand commonalties & differences between data privacy & data security
- ❑ Understand drivers influencing data breach costs
- ❑ Learn about ransomware: avg. ransom-demand, mitigations & insurance considerations
- ❑ Follow practical approach to developing "reasonable" cybersecurity posture
- ❑ Understand key legal obligations & operational impacts for complying with California Consumer Privacy Act (CCPA).
- ❑ Understand CCPA exemptions
- ❑ Understand implications of non-compliance with CCPA
- ❑ Learn what's in store with CCPA 2.0 & other state privacy bills
- ❑ Learn practical approach to complying with patchwork of state privacy laws
- ❑ Learn importance of data governance to achieving sustainability & how it is managed across privacy & security

# Privacy Basics

Jan. 28 **Data Privacy Day** celebrated around the world

**Privacy laws facilitate $2.8 trillion international cross-border data flow**

# Terminology

| Term | Meaning |
|---|---|
| **DSARs** | **Data Subject Access Requests** (GDPR term) |
| **DPLC** | **Data Privacy Lifecycle** – notice, collection, purpose, access, use, sharing, & retention / disposal |
| **Data Mapping** | Mapping DPLC **data flow, data inventory & data locations** (resources) |
| **Resources** | **Products/services, processes, software/apps, databases, technologies, systems & external resources** (service providers/3rd parties) containing/involving PI |
| **PbD / PIAs** | **Privacy-by-Design / Privacy Impact Assessments** (DPIA or Data Protection Impact Assessment) |
| **Privacy-by-Default** | **Strictest privacy settings automatically apply** once a customer acquires a new product / service |

# Differences: Privacy vs. Security

| Privacy | Security |
|---|---|
| Consumer focused | Data focused, includes Bus. Confid. |
| Consumer rights & choices | Data protection |
| Notice / transparency (informed) | IP, network & asset protection |
| Legitimate purpose / consent for collection, use, access, sharing & retention (DPLC management) | Confidentiality, integrity & availability |
| ▪ *Authorized access governance* | ▪ *Unauthorized access* |
| Laws, principles, context, reasonable consumer expectations/social norms & risk oriented | Standards & controls oriented |
| Includes security | Does not include privacy |
| Accountability / governance / trust | Often not included in standards |

# What Does This Tell You about the *Different Nature* of Privacy & Security?

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

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

# Ransomware Is Highly Disruptive

- Ransomware attacks are increasingly **more rampant & vicious**
- Average bitcoin demand was **$41,198** in 3rdQtr 2019 (more than *tripled* from 1st Qtr) & ever increasing
- Ransomware riders have **increased cyber-insurance rates** by as much as 25%
  - May be encouraging payouts & thus more ransomware
- Organizations have been **still recovering 30 days later**
- General **cyber hygiene** which we'll talk about & ability to rapidly restore systems
  - Must be regularly testing recoverability of systems
- **Critical to identify early** to mitigate damage

# 2019 Annual Cost of Breach Study

## by the Ponemon Institute

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

| Avg. U.S. Data Breach Cost | | |
|---|---|---|
| 2006 | 2019 | Increase |
| **$3.54M** | **$8.19M** | **130%** *over 14 years* |

# Breach Impacts Can Be Severe

**Avg. 2019 U.S. *total* data breach costs: $8.19M** (32,434 records/Ponemon Inst.)

- ***Operational resource disruption/distraction* risk**
  - **CEOs lost 1-1.5 yrs of productivity winning back stakeholder confidence (interviews)**
- **Regulatory risk**
- **Legal risk**
- **Financial risk: avg. U.S. breach cost *per compromised record*: $242**
  - **Healthcare: $408 / $13.85M** (1.75Xs - highest of any industry for 8th straight year)
  - **Lost sales & business opportunities - 12-22%** avg. **loss in brand value**
- **Brand/reputation risk: *uninsurable* & can be catastrophic to SMBs**
- ***Officer & director liability risk on the rise***

***How many total consumer records do you have?***

# Breach Cost Considerations

- **Lost business cost: 36.2%** **- biggest cost factor last 5 years**

- Chance of experiencing a **data breach within 2 years: 29.6%**

- ***SMBs face disproportionately larger breach costs relative to larger organizations hampering their ability to recover financially***

  - **Largest organizations** (25,000+ employees) averaged **$204 per employee**

  - **SMBs** (500 - 1,000 employees) averaged **$3,533 per employee**

# *General Factors Affecting avg. Breach Cost per Record*

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

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

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

**Ponemon Institute's 2019 Cost of a Data Breach Study**
507 companies (64 in U.S.) studied that experienced a breach in last year & 3,211 individuals interviewed
https://www.ibm.com/downloads/cas/ZBZLY7KL

# *Factors **Decreasing** avg. Cost per Record*

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

*Companies **without automated incident detection & response** had **95% higher costs***
Cost decreases are **based on global costs**, *so **U.S. cost savings would be greater***

# *Factors* ***Increasing*** *avg. Cost per Record*

| Cost Amplifiers | $ |
|---|---:|
| **Third-party breach** | $370,000 |
| **Compliance failures** | $350,000 |
| **Extensive cloud migration** | $300,000 |
| **System complexity** | $290,000 |
| **OT infrastructure** | $260,000 |
| **Extensive use of mobile platforms** | $240,000 |
| **Lost or stolen devices** | $180,000 |
| **Extensive use of IoT devices** | $160,000 |
| Rush to notify | $150,000 |
| Consultants engaged | $110,000 |

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

# Long Tail Breach Costs

- In a sample of 86 companies -
  - Average of **67% of costs incurred within 1st year**
  - **22%** of costs incurred in **2nd year**
  - **11%** of costs occur **more than 2 years after** data breach
- Organizations in **high regulatory environments experienced a longer tail**
  - 53% in 1st year
  - 31% in 2nd year
  - 16% more than 2 years after incident

# Ponemon: Recommendations to Help Minimize Financial Consequences of a Data Breach

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

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

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

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

- ❑ **Invest in governance, risk management & compliance programs**

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

# CCPA *Powerfully Boosts Class Action Risk*

When "**nonencrypted and nonredacted**" PI is "subject to an **unauthorized access and exfiltration, theft, or disclosure**

as a result of the business's **violation of** the **duty** to implement and maintain **reasonable security** procedures and practices

**appropriate to** the **nature of the information** to protect the information"

# Private Right of Action's PI Definition

*More limited scope of PI were it to be compromised could lead to reportable breach*

- **Private right of action applies to breach of** the following (when not encrypted or redacted):
  - **1st name/initial & last name** *in combination with*:
    - Gov't identifiers: SSN; driver's license # or CA ID card #; Tax ID #; passport #; military ID #; etc.
    - Financial account #; credit/debit card # (in combination with required security/access code or password)
    - Medical info; health insurance info
    - Biometric data generated from measurements or technical analysis of human body characteristics (e.g. fingerprint, retina, or iris image) used to authenticate a specific individual
      - specifies that for breaches involving biometric data, the reporting entity must provide "instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on [that] data for authentication purposes"
  - **Username/email address** *in combination with* **password or security question & answer** permitting access to online account

# Data sensitivity drives a risk-based approach

Determines strength of controls based on data sensitivity levels

| Quartile | 4 Data Sensitivity Classifications | Examples |
|---|---|---|
| 4 | Highly Sensitive | 1st name/initial & 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<br>username/ID or email address w/password or common security question answers (mother's maiden name, DOB, place of birth)<br>financial acct # or payment card info plus any required security/access code or password |
| 3 | Sensitive | 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 |
| 2 | Slightly Sensitive | 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") |
| 1 | Non-Sensitive | non-personal information, such as session identifiers/cookies |

Examples – adjust processes based on data sensitivity levels, e.g. pre-contract due diligence and periodic monitoring of BAs, roles-based access controls (RBAC)

# “Reasonable” (& Defensible) Security

- ***96-99% of breaches avoidable*** by simple & intermediate controls (Verizon DBIRs)
- Select **comprehensive set of standards: ISO 27001-2:2013 + Top 20 CSCs**
  - **CA State AG Office’s** Feb. 2016 CA Data Breach Report: “failure to implement all the **Top 20** (**Critical Security**) **Controls** that apply … constitutes a lack of reasonable security” and “**define(s) a minimum level of information security** …”
    - *Matches well with root causes of breaches*, but **is not a comprehensive framework**
- **Ohio**: 1st state to pass cybersecurity **safe harbor law inoculating businesses *proving compliance*** to recognized security standards

# Top 20 Critical Security Controls v.7.1 (4/01/2019)

**Matches well with *common root causes* of breaches & is updated every couple of years**

## Basic CIS Controls

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

## Foundational CIS Controls

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

## Organizational CIS Controls

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

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

https://www.cisecurity.org/controls/

# NY's SHIELD Act Defines *Reasonable Security* effective 3/2020

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

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

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

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

# Reasonable Security: FTC‘s Data Security Orders

❑ 2019 New and improved data security orders

- **Specific requirements**
- Increase third-party **assessor accountability**
- Elevate data security considerations to **C-Suite & Board**

https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance

# ‘‘Reasonable’’ (& Defensible) Security

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

# Cyber Insurance *Limited in Protections*

- No established standards, so policies vary widely

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

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

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

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

# Mature Privacy Programs Experience Higher ROI

## *Getting $270 on $100* ***is probably one of better investments you can make***

Cisco study - "From Privacy to Profit: Achieving Positive Returns on Privacy Investments“

- ❑ Benefits
  - **Reduces business development delays**
  - **Mitigates losses from data breaches**
  - **Enables agility & innovation**
  - **Makes company attractive to investors**
  - **Builds customer loyalty & trust**
  - **Achieves operational efficiency from data controls**
- ❑ Progress rated: Centre for Information Policy Leadership's Accountability Wheel (1-5 scale)
  1. Leadership & Oversight
  2. Risk Assessment (including DPIA)
  3. Policies & Procedures (including Fairness & Ethics)
  4. Transparency
  5. Training & Awareness
  6. Monitoring & Verification
  7. Response & Enforcement
  - Biggest ROI discrepancies based on **maturity** of organization's privacy program (not co. size)
    - *$2.70 ROI for every $1 spent for companies **rated 1-3*** (U.S. $2.60, UK $3.50, $1.9 lowest)
    - *$3.10 ROI for companies **rated 4+***

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

# California

## Consumer Privacy Act of 2018, Amendments & Regulations (CCPA)

# Background: CCPA & GDPR

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

- ❑ **CCPA – *not comprehensive* & lacks some clarity**
  - *Negotiated in less than a week to **avoid ballot initiative***
  - Published 1.5 years in advance of enforcement
  - But is a *continually moving* target

# CCPA Is *Continually Evolving*

***Privacy Notices, P&Ps and Training* Require *Frequent Updating* to Comply**

- □ **CCPA v1.3**
  - **Amended** in 2018 & 2019
  - ***Other bills*** under consideration will likely amend CCPA
  - CA AG released ***draft* regulations** Oct. 10 prior to 2019 amendments
    - 4 public hearings Dec. 2, 3, 4 & 5
    - 45-day comment period ended Dec. 6
    - Final regulations likely by **spring/summer 2020**
      - ***Updated*** *to include* ***comments & 2019 amendments***
  - ***One additional regulation*** *required by CCPA* ***in 2020***
  - *AG has* ***general rulemaking authority***
- □ **CCPA v2.0** – CA fall ballot initiative will further strengthen CCPA

# CCPA: Accountability Model for Privacy

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

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

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

# CCPA Applicability & Impact

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

- Applicable to "for profit businesses" (data controllers)
  - Greater than **$25M in gross annual revenue**,
  - Annually handle PI of **50,000+ consumers or households**, or
  - **Derive 50%** or more of annual **revenue from "sales" of PI**
- Applies to many SMBs (IAPP estimates):
  - **500,000+ U.S.** & **135,000+ CA businesses**
    - *Underestimates impact on smaller downstream businesses*
- **137 unique CA website visitors/day** = 50K CA consumers
  - Collecting data **via cookies** is within broad definition of PI

# CCPA: Who Is Protected?

- ❑ **Consumers: natural persons who are CA residents** (*customer business relationship not necessary*) including:
  - Company visitors, tenants, students, parents, children, etc.
  - ***Employees/independent contractors & job applicants***
  - ***BTB contact individuals***

- ❑ Scope: **entities processing data from CA consumers, including employers**
  - ***Regardless of whether*** firm *is* ***physically located in CA***

# *Enforcement with Large* ***Civil Penalties***

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

# Right to Sue for *Large Civil Damages*

- Individuals can bring **a civil action**
  - ***Greater of*** **statutory damages of $100-$750 or actual damages** per *consumer per incident* *(<u>$75M</u>/100,000 consumers)*
  - **Applies only to "data breach" violations** & not technical violations of Act as a whole
    - ***Definition of breached PI is narrower*** *than CCPA's PI definition*
  - If consumer provided **30-day written notice & business has not** provided "express written statement" that violation is cured & "no further violations (will) occur"
    - ***Can sue if*** *business* ***continues to violate*** *based on written statement*
  - **For actual** (quantifiable) **damages**, **no notice required**

# CCPA: Incredibly Broad Definition of PI

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

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

Also: gov't public records including PI; records containing PI under FERPA (student privacy)

# CCPA: Incredibly Broad Definition of PI

| 11 categories of PI to extent identify, relate to, describe, are capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer *or household* | |
|---|---|
| **Unique persistent identifiers** that recognize a consumer or family ***over time & across*** different services | **device identifier**; IP address; **cookies**, beacons, pixel tags, mobile ad identifiers & similar technology, customer#, unique pseudonym or user alias; other forms of persistent or **probabilistic identifiers** used to identify a particular consumer or device |
| **Geolocation data** | precise geolocation can be highly sensitive data |
| **Audio, electronic, visual, thermal, olfactory or similar information** | voice recordings, transcriptions, keystrokes, etc. |
| **Professional or employment-related information** | job applicants, benefits, compensation, performance reviews, education/resume (one-year moratorium) |
| **Inferences drawn** | **profile** of preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities & attitudes |

Also: gov't public records including PI; records containing PI under FERPA (student privacy)

# CCPA: Aggregate & De-identified Data Is **Not PI**

| Information | Meaning |
|---|---|
| **Aggregate** | information that relates to a **group or category** of consumers, from which individual consumer identities have been removed and is "**not reasonably linkable" to a** consumer or household<br>(**household** means a person or group of persons occupying a single dwelling) |
| **De-identified** | information that **cannot reasonably** *identify, relate to, describe,* be ***reasonably capable of being associated with***, ***or be linked***, directly or **indirectly**, to a particular consumer (*eliminates "key-coded" data*) |

CCPA requires **4 safeguards** to **prohibit/prevent reidentification**

# CCPA: 4 Required Safeguards to Prevent Reidentification

1. **Implement technical safeguards prohibiting reidentification**
   a. Collaborate with qualified statistician to establish enterprise-wide deidentification rules for the removal of certain PI data types.

2. **Implement business process specifically prohibiting reidentification**
   a. Develop an internal policy/procedure preventing employees and service providers (include in addendum) from attempting to reidentify data.

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

4. **Make no attempt to reidentify the information**
   a. Properly sanction personnel who violate policies enacted to prohibit reidentification

# Don’t Use Terms: Anonymous or Anonymized

*Recent study published in Nature Communications -*

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

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

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

Source: https://www.jdsupra.com/legalnews/is-anonymized-data-truly-safe-from-re-55837/

# CCPA Privacy Notices Practices

***Many specific requirements for notices / statutory penalties for failure to disclose***

- ❑ Privacy notice availability
- ❑ **Data mapping** facilitates accurate privacy notices
- ❑ **Privacy notice frequency of update** requirements
- ❑ **Cookie policy**
- ❑ General privacy notices readability requirements
- ❑ **4 Types of Consumer Notices**
  - Just-in-time notice at/before time of collection of PI
  - Just-in-time notice of financial incentive(s)
  - Notice of right to opt-out of sale of PI
  - Privacy notice with specific rights and other disclosures

# Cookie (basics) policy

- □ **Conduct cookie audit** (open source tools)

- □ Identify/**deactivate non-essential** persistent cookies (not necessary for performance of website functionality, ecommerce)

- □ **Inform online privacy notice**'s disclosures

- □ **Inform just-in-time notice**/disclosure & express opt-in
  - **No pre-checked boxes**
  - **No implied consent** by continuing to use site (EU)
  - **No website blocking** after refusing to accept cookies (EU)

# Data Mapping Is Critical for Data Discovery & Inventory and Rights Management

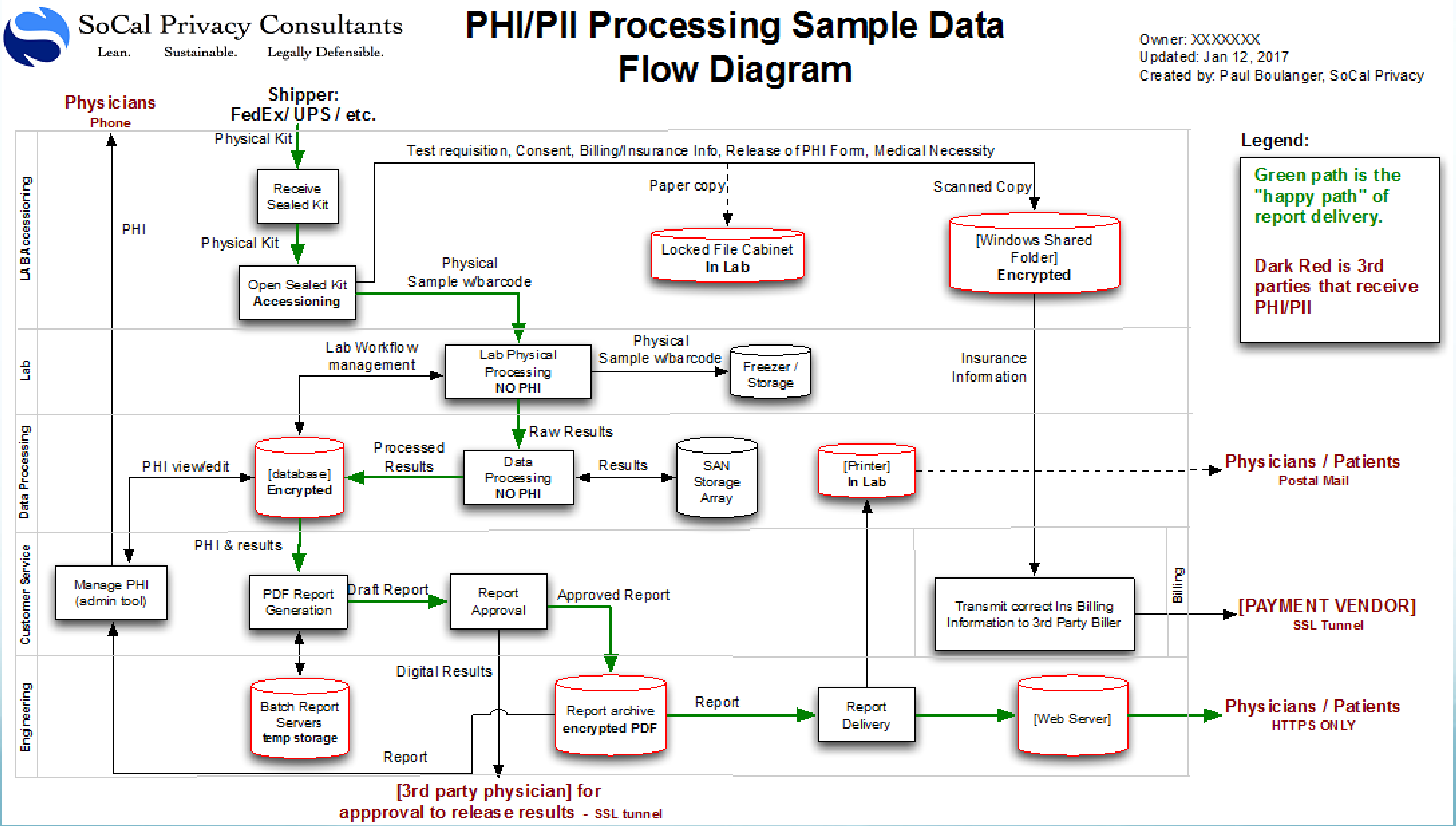
- □ **Data map** & update immediately:
  - Before Jan. 1, 2020
  - ***Annually thereafter*** (12 mo. lookback)
  - Before any changes to data types collected or its use and other required notice disclosures

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

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

# Sample Data Flow Diagram

*Our Data Mapping whitepaper is in IAPP's Resource Center available to 50,000+ global members*



SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

## PHI/PII Processing Sample Data Flow Diagram

Owner: XXXXXXX
Updated: Jan 12, 2017
Created by: Paul Boulanger, SoCal Privacy

Legend:

Green path is the "happy path" of report delivery.

Dark Red is 3rd parties that receive PHI/PII

# Resource & Data Inventory

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

**Data Resource Map**: ________________ (Name of DPLC)
**Document Owner**: ________________ **Rev Date**: __________

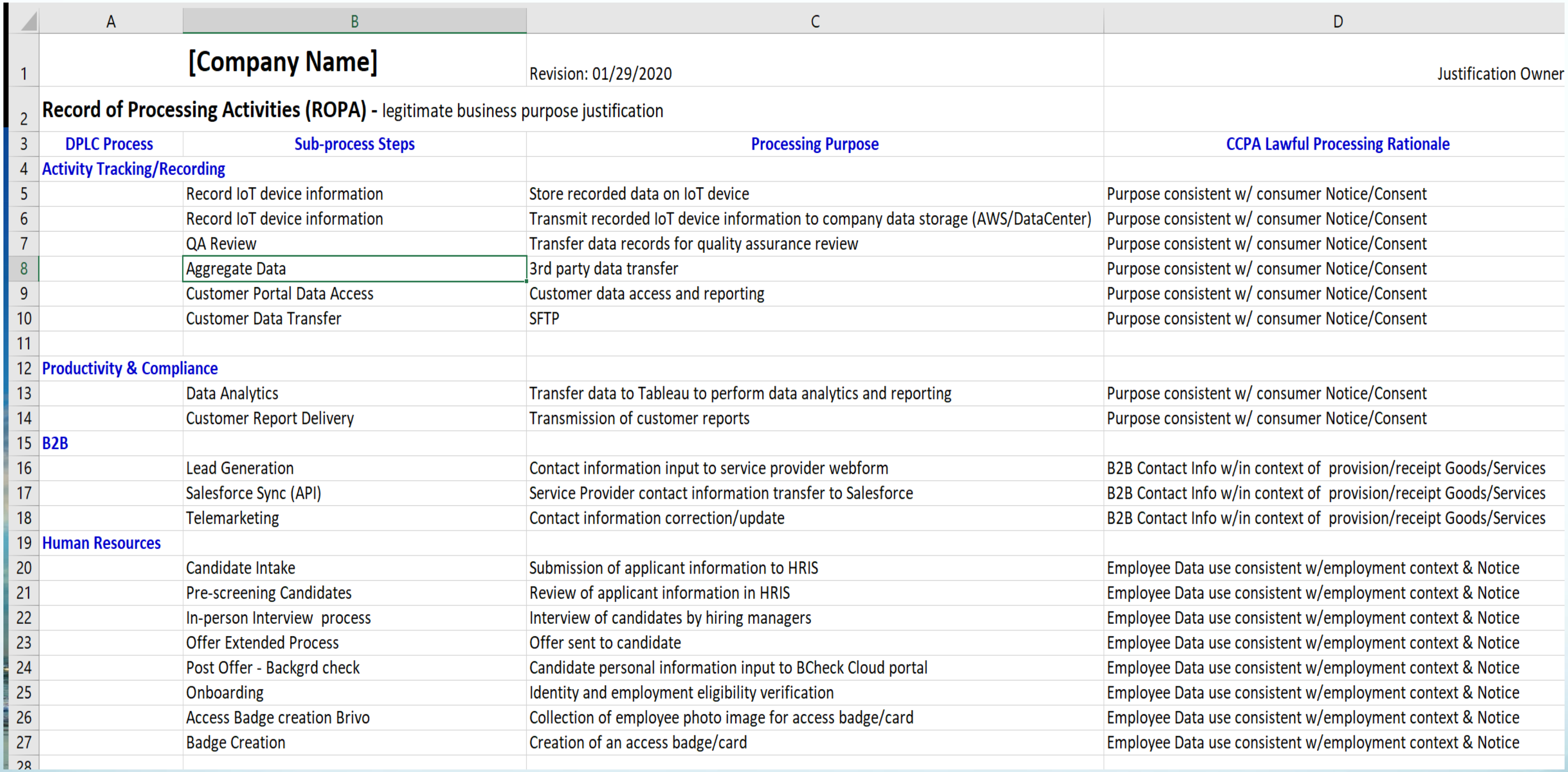
**Also create a service provider & third party inventory**

| Data Locations | Database | Shared folder | Box | Share Point | File cabinet | AWS S3 |
|---|---|---|---|---|---|---|
| **Resource owner** | J Dunbar | J Dunbar | A Spellman | J Dunbar | J Dunbar | A Spellman |
| **Resource custodian** | M Marks | P Mann | C Grant | P Mann | D Rossi | M Mitchel |
| **Data inventory** | | | | | | |
| • **Data identifiers** | Acct#, DL#, Name, Password | Photo, Name | Acct#, Name, GPS | Device ID, Name | Name, Address, Signature | Acct#, Name, PW, Photo, Device ID |
| **Classification** | | | | | | |
| • Highly sensitive | X | | X | | | X |
| • Sensitive | | | | X | | |
| • Slightly sensitive | | X | | | X | |
| • Non-sensitive | | | | | | |

- **Develop at the end of data mapping session** – add as many columns / rows of columns as necessary
- **List all data identifiers** for each resource
- **Identify highest data sensitivity level** which determines required strength of controls

# Process Inventory Analysis

## *Akin to Record of Processing Inventory* (ROPA) *Required by GDPR*



| | A | B | C | D |
|---|---|---|---|---|
| 1 | | **[Company Name]** | Revision: 01/29/2020 | Justification Owner |
| 2 | **Record of Processing Activities (ROPA) -** legitimate business purpose justification | | | |
| 3 | **DPLC Process** | **Sub-process Steps** | **Processing Purpose** | **CCPA Lawful Processing Rationale** |
| 4 | **Activity Tracking/Recording** | | | |
| 5 | | Record IoT device information | Store recorded data on IoT device | Purpose consistent w/ consumer Notice/Consent |
| 6 | | Record IoT device information | Transmit recorded IoT device information to company data storage (AWS/DataCenter) | Purpose consistent w/ consumer Notice/Consent |
| 7 | | QA Review | Transfer data records for quality assurance review | Purpose consistent w/ consumer Notice/Consent |
| 8 | | Aggregate Data | 3rd party data transfer | Purpose consistent w/ consumer Notice/Consent |
| 9 | | Customer Portal Data Access | Customer data access and reporting | Purpose consistent w/ consumer Notice/Consent |
| 10 | | Customer Data Transfer | SFTP | Purpose consistent w/ consumer Notice/Consent |
| 11 | | | | |
| 12 | **Productivity & Compliance** | | | |
| 13 | | Data Analytics | Transfer data to Tableau to perform data analytics and reporting | Purpose consistent w/ consumer Notice/Consent |
| 14 | | Customer Report Delivery | Transmission of customer reports | Purpose consistent w/ consumer Notice/Consent |
| 15 | **B2B** | | | |
| 16 | | Lead Generation | Contact information input to service provider webform | B2B Contact Info w/in context of provision/receipt Goods/Services |
| 17 | | Salesforce Sync (API) | Service Provider contact information transfer to Salesforce | B2B Contact Info w/in context of provision/receipt Goods/Services |
| 18 | | Telemarketing | Contact information correction/update | B2B Contact Info w/in context of provision/receipt Goods/Services |
| 19 | **Human Resources** | | | |
| 20 | | Candidate Intake | Submission of applicant information to HRIS | Employee Data use consistent w/employment context & Notice |
| 21 | | Pre-screening Candidates | Review of applicant information in HRIS | Employee Data use consistent w/employment context & Notice |
| 22 | | In-person Interview process | Interview of candidates by hiring managers | Employee Data use consistent w/employment context & Notice |
| 23 | | Offer Extended Process | Offer sent to candidate | Employee Data use consistent w/employment context & Notice |
| 24 | | Post Offer - Backgrd check | Candidate personal information input to BCheck Cloud portal | Employee Data use consistent w/employment context & Notice |
| 25 | | Onboarding | Identity and employment eligibility verification | Employee Data use consistent w/employment context & Notice |
| 26 | | Access Badge creation Brivo | Collection of employee photo image for access badge/card | Employee Data use consistent w/employment context & Notice |
| 27 | | Badge Creation | Creation of an access badge/card | Employee Data use consistent w/employment context & Notice |
| 28 | | | | |

# ***CCPA Basic Consumer Rights***

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

- ❑ Right to **know**
  - ***Privacy notice***
  - ***Just-in-time notice*** *with abbreviated disclosures at or prior to collection*
- ❑ Right of **access & data portability**
- ❑ Right to **request deletion** with certain exceptions
- ❑ Right to **opt-out of "sale"** of PI & for children to opt-in
- ❑ Right to **equal service/price** (anti-discrimination) for exercising rights

# Other CCPA Internal Business Impacts

❑ **Also data map & establish governance around these DPLCs,** e.g. establish resource owners/custodians, honor rights, etc:

- **BTB Contact Information** (CRM: marketing, sales & bus dev)
  - **1-year moratorium** for data involving providing/receiving a product/service or due diligence
  - Must still comply with **Do Not Sell** obligations
  - **Private right of action** still available for breaches
  - Carve-out does not affect marketing communication or other BTB communications that do not involve receiving/providing a product/service

- **Employee Data**
  - **1-year moratorium** for data **used in employment context**
  - **Employee privacy** notice still required (includes job applicants)
  - **CCPA applies** for employee data used **outside employment context**
  - **Private right of action** still available for breaches – *evaluate security*

# CCPA Exemptions Not All Encompassing

General applicability, independent of industry sector with certain exceptions

- ❑ **Non-profits with exceptions**

- ❑ **Federal privacy laws**
  - **HIPAA/CMIA** covered entities (CEs) – not BAs at this time
    - ***PI*** *(defined by CCPA) exempted to extent* ***treated in same manner as PHI***
  - **Federal "Common Rule" clinical trials** following certain good clinical practice guidelines
    - *Excludes research for* ***commercial purposes*** *– bill may change this*
  - **GLBA** entities
    - *Are subject to CCPA when engage in* ***activities outside of GLBA***
  - **FCRA & DPPA**

# CCPA Service Provider & Third Party Management

| Term | Meaning |
|---|---|
| **Service Provider**<br>– Subcontractors | An entity that ***receives PI from*** **a data controller & processes that PI strictly on behalf of** data controller ***pursuant to certain contractual terms***. For any entity to be considered a service provider, it **must agree to certain contractual restrictions** or by default it becomes a data controller or third party with greater obligations. Thus, service providers **should** either **sign a proper CCPA Service Provider Addendum** or agree to update the master services agreement to incorporate these restrictions. |
| **Third Party**<br>– Ad networks, data brokers, social networks & data analytics providers | **Any other person/entity**, other than a data controller or service provider, **receiving PI** from and under control of data controller or service provider. **When valuable consideration is involved**, a "Do Not Sell My Personal Information" or "Do Not Sell My Info" opt-out ("**opt-out**") link must be offered. *Given CCPA's definition*, third party takes on **a different meaning** than how it has been used in the past and does not include service providers.<br>▪ **2020 CA ballot initiative**: **opt-in** for PI sold or used for advertising purposes<br>▪ Organizations are moving away from behavioral ads to **contextual ads**<br>▪ Follow ad self-regulatory agencies, e.g. **Interactive Advertising Bureau (IAB)** |

# Mature CCPA Privacy Program P&Ps

- ❑ **Privacy Operations** Practices
- ❑ **Privacy Notices** Practices
- ❑ Privacy **Choice & Consent Practices**
- ❑ Consumer Rights Requests (**DSARs**)
  - DSAR Submission & Verification
  - DSAR Coordination, Timeframes, Response & Record-keeping
  - DSAR Disclosure Fulfillment Requirements
  - DSAR Request Webform
- ❑ **Service Providers & Third Parties** Management
  - CCPA Service Provider Addendum
- ❑ **Employee Data** Privacy Practices
- ❑ **B2B Contact Information** Privacy Practices
- ❑ **Training** Program

# Highlights: How CCPA 2.0 Expands CCPA

**Effective Jan. 1, 2021** *with deadline for final regulation one year later*

- ❑ **Bumps threshold:** buying/selling/sharing/collecting PI **to 100,000+** CA consumers (274/day)
- ❑ 12-month disclosure extended over more periods as long as isn't unduely burdensome
- ❑ New **California Privacy Protection Agency** enforces privacy laws & impose fines
- ❑ Requires disclosure of use of **automated decision-making** (performance at work, economic situation, heath, personal preferences, etc.) & allows **certain opt-out rights** with respect to such use
- ❑ Creates **sensitive PI category** (sex life/sexual orientation, private communications, health status, geolocation, religion, race, finances, biometrics, etc.)
  - CA consumers receive **enhanced rights**, e.g. **opt out** of its use **in marketing/advertising**
- ❑ Creates additional protections for PI of children, including $7,500 fine for violations if have actual knowledge that affected consumer is **under 16 years of age**
- ❑ Mandates further disclosure obligations & reinforces must follow own disclosures
- ❑ Must **disclose reasons** for types & amount of PI collected & **how long retained** (GDPR-like)
- ❑ **Specifies** use of PI for purposes other than those disclosed, retained for longer than stated, or collected more information than was needed to offer relevant service/product would be in **violation**

# CCPA's Key Operational Impacts

- ❑ Apply CCPA with **CA residents only** or across the U.S?
- ❑ Grasping expanded **PI definition**, 11 PI categories & covered data set
  - ***Deidentification rules*** *may require qualified statistician validation*
- ❑ Establishing **clear roles & responsibilities** for privacy governance
  - *Privacy Official, DSAR Coordinator, Resource Custodian, etc.*
- ❑ Heavy **roles-based training** of many different groups
  - *Awareness training alone will not operationalize CCPA compliance*
- ❑ Creating & maintaining **data mapping** before changes occur
  - *Requires DPLC process owner role & responsibilities*
- ❑ Maintaining **accurate**/real time **privacy notices** & just-in-time notices
  - *Including employee/job applicant privacy notice*
  - Actively manage & account for **cookies** in notices

# CCPA’s Key Operational Impacts

- ❑ Providing appropriate **opt-outs/ins, suppression & tracking**
  - Determining when **PI** is “**sold**” (valuable, not monetary, consideration)
- ❑ Operationalizing **DSAR** process – deletion, portability, etc.
  - DSAR designated methods for submission & verification requirements
    - **Authorized agents** registered with CA
  - DSAR coordination, timeframes & record-keeping requirements
  - DSAR disclosure fulfillment requirements
    - **Unstructured data & household data**
- ❑ Anti-discrimination requirements for discounted products/services
- ❑ Properly managing **service providers & third parties**
- ❑ Qualifying for exemptions: HIPAA, GLBA, etc.
- ❑ Protecting crown jewels with “**reasonable security**” (increased class action risk)
- ❑ **Complying** with final/future regulations, future amendments & CCPA 2.0

# In Sum

- ❑ State of perpetual & every increasing **cyber warfare**
- ❑ **Social media** hammers the ill-prepared
- ❑ **Class action lawsuits** on the rise
- ❑ **Statutory penalties** for violations
- ❑ **Compliance** alone is not enough
- ❑ **Cyber insurance** may provide partial or no coverage
- ❑ Willful neglect or **good-faith** efforts?
- ❑ Privacy & security are **business risks & objectives** (not compliance risks)

# Be Prepared!

- ❑ **Business partner and M&A due diligence** requirements
  - **CCPA** requirements
  - Increasing cybersecurity requirements
- ❑ Early adopters have **competitive advantage**
- ❑ **Part of Trust equation**:
  - Privacy is a customer expectation
  - Thus, Privacy/Security-by-Design is a **functional requirement** of services, products, processes, etc.
- ❑ Requires **defensible & sustainable program** of policies/SOPs, governance & embedded practices

# Mature Program
# Sustainability Requirements

# Mature Program Requires Sustainability

- **Sustainable** (NIST: repeatability)
  - Most clients have **ad-hoc or risk informed** practices
  - Goal: establish **repeatable** practices based on
    - *Demonstrated* **executive commitment and support**
    - **Governance with clearly defined roles and responsibilities** for oversight, execution and monitoring
    - **Requires *organizational, cultural & operational changes***
    - Program ***matures over time***, not a short-term project (3-5 years)
- **Defensibility**: build proactive **risk management & Privacy/Security-by-Design processes** on top of compliance
  - *Check-the box compliance is not enough*

# Mature Privacy Program Elements

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

# Foundational Program Governance

*Next slides include operational recommendations for governance elements*

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

External Resource Management means governance of **service providers & 3rd parties** under CaCPA
Other related governance scopes include *M&A, outsourcing, system architecture, change management, project management, etc.*

# Privacy Bills in Progress

***Imagine** patchwork of 50 state privacy laws (akin to breach notification laws)*

## Modeled on CCPA

- Hawaii
- Maryland
- Massachusetts
- New Mexico
- Rhode Island
- Connecticut
- New York
- Pennsylvania
- Texas

## Varies more with CCPA

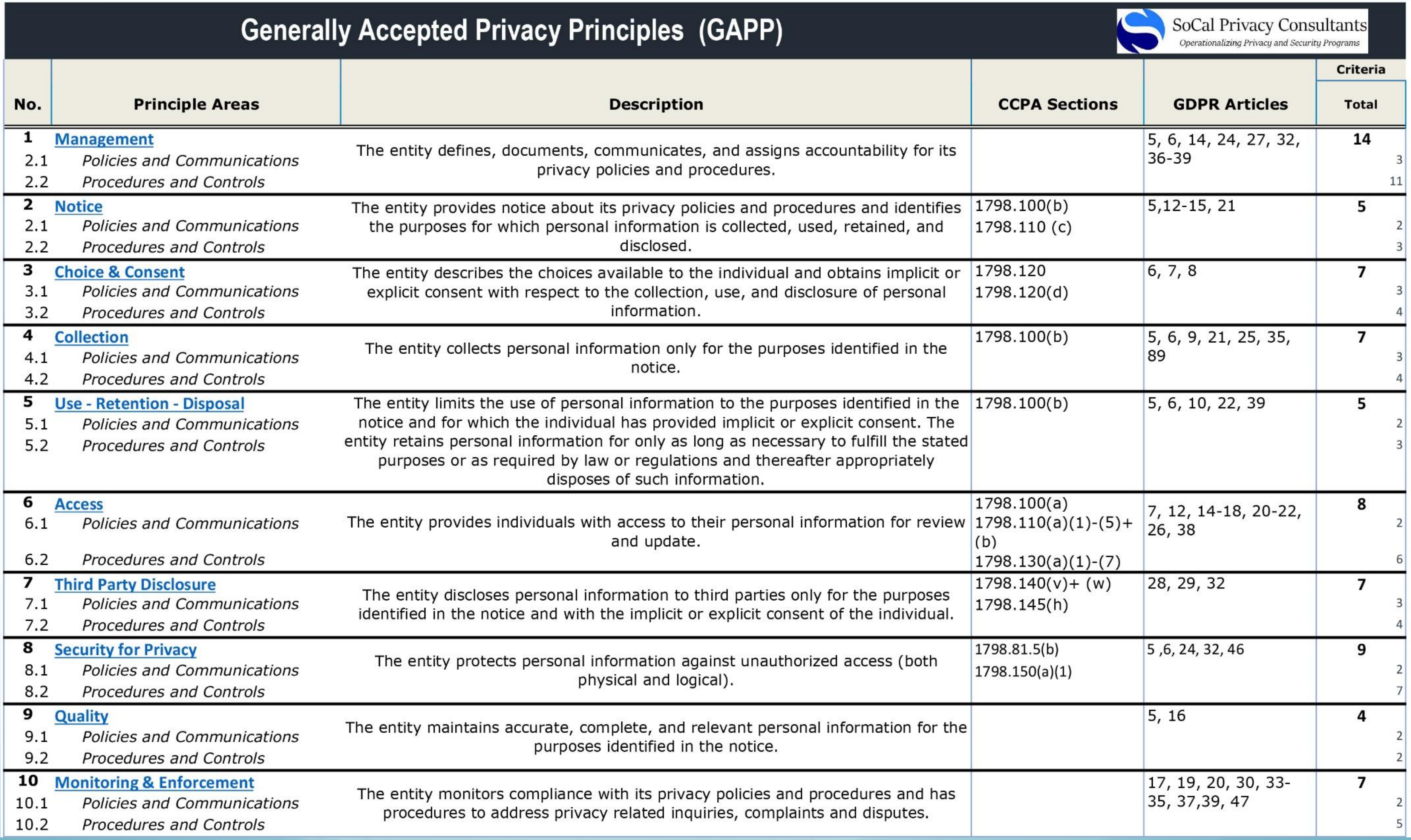
- Illinois
- New Jersey
- New York
- Oregon
- Virginia
- Louisiana
- Nevada: *effective **10/1/19** – **Sale Opt-out***
- Washington

# Federal Privacy Law?

- *Tech giants pushing for* ***U.S. omnibus privacy law*** ***to preempt state law & without private right of action***
  - Congress appears too dysfunctional to act
  - Many states would sue to prevent preemption & may win
  - Not likely going to achieve EU’s “adequacy” standard
- *Don’t hold your breadth –* ***be prepared to comply with a patchwork of state laws***

# Integrate CCPA into GAPP Privacy Principles

## *Requires data governance to enforce these principles* ***(AICPA/CICA)***



Generally Accepted Privacy Principles (GAPP)

SoCal Privacy Consultants
Operationalizing Privacy and Security Programs

| | | | | | Criteria |
|---|---|---|---|---|---|
| **No.** | **Principle Areas** | **Description** | **CCPA Sections** | **GDPR Articles** | **Total** |
| **1** | **Management** | The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures. | | 5, 6, 14, 24, 27, 32, 36-39 | **14** |
| 2.1 | *Policies and Communications* | | | | 3 |
| 2.2 | *Procedures and Controls* | | | | 11 |
| **2** | **Notice** | The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed. | 1798.100(b)<br>1798.110 (c) | 5,12-15, 21 | **5** |
| 2.1 | *Policies and Communications* | | | | 2 |
| 2.2 | *Procedures and Controls* | | | | 3 |
| **3** | **Choice & Consent** | The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information. | 1798.120<br>1798.120(d) | 6, 7, 8 | **7** |
| 3.1 | *Policies and Communications* | | | | 3 |
| 3.2 | *Procedures and Controls* | | | | 4 |
| **4** | **Collection** | The entity collects personal information only for the purposes identified in the notice. | 1798.100(b) | 5, 6, 9, 21, 25, 35, 89 | **7** |
| 4.1 | *Policies and Communications* | | | | 3 |
| 4.2 | *Procedures and Controls* | | | | 4 |
| **5** | **Use - Retention - Disposal** | The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. | 1798.100(b) | 5, 6, 10, 22, 39 | **5** |
| 5.1 | *Policies and Communications* | | | | 2 |
| 5.2 | *Procedures and Controls* | | | | 3 |
| **6** | **Access** | The entity provides individuals with access to their personal information for review and update. | 1798.100(a)<br>1798.110(a)(1)-(5)+ (b)<br>1798.130(a)(1)-(7) | 7, 12, 14-18, 20-22, 26, 38 | **8** |
| 6.1 | *Policies and Communications* | | | | 2 |
| 6.2 | *Procedures and Controls* | | | | 6 |
| **7** | **Third Party Disclosure** | The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. | 1798.140(v)+ (w)<br>1798.145(h) | 28, 29, 32 | **7** |
| 7.1 | *Policies and Communications* | | | | 3 |
| 7.2 | *Procedures and Controls* | | | | 4 |
| **8** | **Security for Privacy** | The entity protects personal information against unauthorized access (both physical and logical). | 1798.81.5(b)<br>1798.150(a)(1) | 5 ,6, 24, 32, 46 | **9** |
| 8.1 | *Policies and Communications* | | | | 2 |
| 8.2 | *Procedures and Controls* | | | | 7 |
| **9** | **Quality** | The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice. | | 5, 16 | **4** |
| 9.1 | *Policies and Communications* | | | | 2 |
| 9.2 | *Procedures and Controls* | | | | 2 |
| **10** | **Monitoring & Enforcement** | The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes. | | 17, 19, 20, 30, 33-35, 37,39, 47 | **7** |
| 10.1 | *Policies and Communications* | | | | 2 |
| 10.2 | *Procedures and Controls* | | | | 5 |

# Eight Questions to Ask

1. What **security framework** is our security program and policies/SOPs based on? E.g. ISO 27001-2:2013

2. Do the security program and policies/SOPs also address the **Top 20** Critical Security Controls as appropriate to comply with CA law?

3. **How quickly** can we **recover** from a ransomware attack if it were to lockup all databases?

4. Have we **mapped** our data flows and inventoried our resources and the data contained therein? Have owners been established to **maintain** future states?

5. Has our consumer-facing **privacy notice** been updated to comply with CCPA?

6. If we sell or plan to sell PI, is the **"Do Not Sell My Personal Info" link** setup?

7. Do we have **internal CCPA policies**?

8. Do personnel **understand** that no new PI can be collected and no existing PI used or shared for a different purpose until the privacy notice is first updated?

9. Do we have a **consumer access rights process and tracker** set-up and has it been tested?

**If You Haven't Started to Comply,**
***Don't Wait*** **–**
**Every Day of Delay Falls on the**
***Willful Neglect*** **Side of the Ledger –**
**Better to** ***Begin Good Faith Efforts Now***

# So much more … let us know if questions about -

- **Artificial Intelligence** risks & transparency
- **IoT** risks, laws & security frameworks – CA & OR with 5 bills in other states; NIST & ENISA (EU)
  - E.g. smart building systems are vulnerable to attack (doors, elevators, HVAC, etc.
- **Biometrics** laws & class actions – Illinois & other states
  - **Facial recognition** risks & technology
- **Automated decision-making/profiling** risks & transparency

# ANY FINAL QUESTIONS?

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

**Michael Cox, CIPP/US**
mcox@socalprivacy.com
619.318.1263
**Neil R Packard, CISA**
npackard@socalprivacy.com
619.208.2529
www.socalprivacy.com

SoCal Privacy Consultants
*Operationalizing Privacy and Security Programs*

# Appendix

Supplemental Information<br>
About Us

# IAPP Certifications

https://iapp.org/certify/programs/

- □ **The "what" of privacy laws & regulations**
  - **CIPP/US**
  - **CIPP/E** – EU (GDPR)
  - **CIPP/C** – Canada
  - **CIPP/A** - Asia
- □ **The "how" of privacy operations**
  - **CIPM** – Certified Information Privacy Manager
- □ **The 'how' of privacy & technology**
  - **CIPT** – Certified Information Privacy Technologist (PbD)

# 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?*

***Experience*** *– major law firms still recommend the Big Four, but choose us when 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 and also as an enterprise risk management officer for a top 10 bank*
  - *Neil has security audit, IT director and e-discovery experience as well as 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 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: 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

- ❑ **Work tools** – *Also delivered for your reuse*
  - **Data mapping: SIPOC & resource/data inventory** (Excel) with example interview questions
  - **Controls evaluations workbooks** (Excel) that include a tab *identifying gaps*
  - **Risk assessment workbook** (Excel) **& placemat** (valuation methodology)
    - *Documents entire process and provides instructions for repeatability*
  - **Requested documents list** (Word) used post-assessment to evaluate readiness

- ❑ **Deliverables**
  - **Data Flow Diagram(s)** (Vizio) – current & if planned changes - future states
  - **Privacy Impact Assessment** (PIA) **Report** of recommendations (Word)
  - **Security Summary Report** (Word)
  - **Risk Register** of *risks identified during the risk assessment* (Excel)

Recommend setting up a shared, but restricted **compliance repository** for all documentation to facilitate governance/oversight and being prepared to promptly respond to information requests and investigational demand letters

SoCal Privacy Consultants

*Operationalizing Privacy and Security Programs*

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 – Assessment

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

Phase 2 – Implementation Support as requested, including polices and procedures

- 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
CEO 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

# Comparing CCPA to EU's GDPR

## And HIPAA & GLBA Impacts

# Commonalities: CCPA & GDPR

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

# Key Differences

*Compliance can be leveraged, but recognize differences*

## CCPA

- **Business applicability thresholds**
- **11 Categories of PI**
- **Informed privacy notice & consumer rights oriented**
- **12 mo. look-back at data collected for disclosure requests**
- **Anti-discrimination**
- **Service provider contractual obligations**

## GDPR

- **Offering goods/services or profiling/monitoring**
- **Personal Data defined broadly**
- **Legitimate purpose analysis**
- **Privacy-by-Design/DPIA**
- **Demonstrable compliance proof**
- **Data retention**
- **Explicit data processor contractual requirements**
- **DPO, local legal representative**
- **X-border data transfer rules**, e.g. PS

*See Appendix for a deeper comparative analysis*

# Rights Similar, But Must Account for Differences

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

Response timeframes, exceptions, & denial reasons are different

# “Reasonable” (& Defensible) Security

- ❑ Select a **comprehensive set of standards**
  - ***96-99% of breaches avoidable*** by simple & intermediate controls (Verizon DBIRs)
- ❑ Identify what is reasonable under the circumstances & **exceptions** based on:
  - Company **size, complexity & capabilities; industry, DTC/BTB; jurisdictions**
  - **Nature & sensitivity of PI**
  - **Technical, hardware & software infrastructure**
  - **Costs of security measures (vs. benefit)**
  - **Probability & impact of likely risks** to PI
  - **Insurance & client due diligence requirements** (Fortune 500)

# "*Reasonable (Defensible) Security*" Requirements

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

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

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

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

- ❑ IoT security standards are rapidly emerging

# Monitoring & Evaluation

## Governance Operational Recommendations

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

- Define activities in policy, assign ownership & timetables
  - Regular, appropriate patching - FTC emphasis
  - Periodic risk assessment & controls evaluation
  - Periodic vulnerability scans & penetration tests
  - Periodic code reviews
  - Periodic RBAC rights review
  - Periodic hardware/software inventory reconciliation
  - Periodic review of access points & wireless
  - Periodic 3rd-party due diligence based on data sensitivity
  - Periodic incident response desktop exercise &/or simulation
  - Periodic testing of Business Continuity & Disaster Recovery plans

# CCPA Corresponding Business Obligations

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

https://www.perkinscoie.com/images/content/2/0/v2/204179/Perkins-Coie-CCPA-White-Paper-Oct.-2018.pdf

# CCPA Privacy Operations Practices

- ❑ Jurisdictional scope: CA only or across the U.S.?
- ❑ **Personal Information definition**
- ❑ **Consumer rights**
- ❑ Anti-discrimination
- ❑ **Deidentified & aggregate data**
- ❑ Highly sensitive data
- ❑ Concept of "reasonable security"

# CCPA: Employee Data & B2B Contact Information

| Term | Meaning |
|---|---|
| **Employee Data** | PI businesses collect from job **applicants, employees**, owners, officers, medical staff, and contractors to the extent the company **uses the PI *solely in the capacity of the person's role with the company, including benefits and emergency contact information*.** There is a **limited one-year moratorium** in terms of full CCPA applicability to such employment data. Businesses are still required to provide **separate privacy notices to job-applicants and employees** (as DPLCs are different) and such personnel still benefit from the **private right of action**. CCPA is **fully applicable to employee data used outside the capacity of the person's role**. |
| **B2B Contact Information** | **PI solely collected and used in B2B company communications and transactions with other companies**, organizations, and government agencies **from or about an employee**, owner, director, officer or contractor of a business or government agency **obtained in the context of due diligence or provision/receipt goods/services**. There is a **limited one-year moratorium** from most CCPA requirements. This exemption **does not apply to the right to opt-out of the sale of PI**, the obligation not to discriminate against a consumer for attempting to exercise their rights, or the **private right of action** in event of a data breach. B2B companies will still have to determine if and to what extent they **must comply with CCPA requirements for other types of PI they collect, such as for marketing purposes with prospective customers.** |

# CCPA Employee Data Privacy Practices

- ❑ Job-applicant & employee **data mapping**

- ❑ Employee data **used within employment capacity**
  - **Separate job applicant & employee privacy notices**

- ❑ Employee data **used outside employment capacity**
  - **Separate employee privacy notice** for data used outside context
  - **Full consumer rights, e.g. DSARs**

- ❑ **HR service providers**, e.g. applicant/recruiting services, etc.
  - Execute CCPA service provider addendum

- ❑ **Employee documents** – update for CCPA's definition of PI
  - Employee handbook, confidentiality agreements, separation agreements, arbitration agreements, independent contractor agreements
  - Disclose any electronic **employee monitoring programs**

- ❑ HR employee data **security polices & procedures** (unstructured data)

# CCPA B2B Contact Information

*Work with Business Development, Sales & Marketing to ensure compliance*

- ❑ B2B contact information **data mapping**
- ❑ **Exempt**: B2B contact information **used within provision/receipt goods/services or due diligence**
  - ***Use for secondary purpose*** **triggers express consent & full CCPA compliance**
- ❑ B2B contact information **used outside context in which provided**
  - **Privacy notice** for data used outside context
  - **Full consumer rights, e.g. DSARs**
- ❑ **B2B service providers**, e.g. Salesforce in the cloud
  - Execute CCPA service provider addendum
- ❑ **Avoid obtaining** B2B contact information **from a data broker which may trigger full CCPA applicability**

# GLBA Entities & CCPA

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

# HIPAA Covered Entities: Qualifying for CCPA Exemption

- □ **Treat Non-Regulated PI Same as PHI**
  - *CCPA provides no specific guidance*
- □ **Include CCPA's PI definition scope in**:
  - **Privacy notices**
  - **Confidentiality agreements**
  - **Privacy & security policies**/SOPs & practices, e.g. AUP
  - **Training**
  - **Business associate agreements** (protection flow down)
  - *Watch for clarification* via rule-making, etc.
- □ **Lots of vagueness**, for example re: ***deidentification rules***

# CCPA Definitions: Devil is in the Details

| Activity | Meaning |
|---|---|
| **Collection** | ***buying, renting, gathering, obtaining, receiving, or accessing*** any PI pertaining to a consumer, ***either actively or passively, or by observing consumer's behavior*** |
| **Sale**<br>(does not mean "sell" as usually understood) | 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/entity*** 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 CCPA, **requiring** disclosure & **opt-out** (opt-in for children)

# 4 Types of **Consumer Notices**

- *Each with specific disclosure requirements*
  - **Just-in-time notice** at/before time of collection of PI
  - **Just-in-time notice of financial incentive(s)**
  - **Notice of right to opt-out** of sale of PI
  - **Privacy notice** with specific rights/other disclosures

# CCPA Privacy Choice & Consent Practices

- **Explicit consent** for purpose **not disclosed** in privacy notice

- Wanting to "sell" PI when not collecting PI directly from consumers – directly contact:
  - Consumers to provide notice of sale of PI & notice of right to opt-out, or
  - Source of PI to confirm provided proper notice at collection & obtain signed attestation describing how notice was given with sample

- **Engineering requirements** for Do Not Sell opt-out & children's opt-in
  - Do Not Sell requirements
  - On-hold pending final reg: ***treat user-enabled browser opt-out/DNT signals***
  - For those not offered opt-out, if later want to sell PI – treat as opted-out & require opt-in to sell PI
  - Children's opt-in requirements
  - Timeframes, tracking & suppression
  - Periodic testing

- **Operational requirements** for Do Not Sell opt-out & children's opt-in
  - Manual DSARs requesting opt-outs/ins
  - **Opt-out DSARs do not need to be verifiable** unless suspect fraud
  - Cannot require to create an account to exercise rights (undue hindrance)

# In Sum: Operationalizing Consumer Rights

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

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

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

# In Sum: Operationalizing Consumer Rights

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

# CCPA Consumer Rights Requests (DSARs)

- Consumer Access Rights Requests (DSARs) Policy
  - **Communication method**
    - **Verbal** whenever verification difficult, to constrain request to PI of concern, & convey unexpected news
    - More efficient, engenders trust & mitigates complaints/enforcement/lawsuits
  - General access policy
    - Provide as much control to consumers over PI as possible
  - **Structured vs. unstructured data**
    - **Use appropriate portal/CRM/repositories** to communicate PI vs. email not intended as a repository & shared folder
- DSAR Submission & Verification and DSAR (Rights Request) Webform
- DSAR Coordination, Timeframes, Response & Record-keeping
- DSAR Disclosure Fulfillment Requirements

# CCPA **DSAR** Submission & Verification

- **Designated methods** for DSAR submission, including opt-out from sale of PI
  - 2+: **toll-free phone#** + method reflecting **primary way** interacts w/ consumer
    - Interactive webform (in draft regulation)
    - Email, mail, in-person (e.g. in-store)
  - **Email address only, if** business has direct relationship w/ consumers solely online

- DSARs submitted in an **alternative manner** for request to know or delete
  - Required: accept or provide specific directions as to how to submit or remedy request
  - Recommend: **accept** written requests (**email/mail**) same as designated method DSARs

- DSAR **submission & receipt**
  - **Consumer contact personnel explain** rights & how to submit requests to consumers
  - **Promptly direct** DSARs **to DSAR Coordinator** (day one counts as receipt)

# CCPA DSAR Submission & Verification

- **General verification** procedures and guidelines
  - **First matching/using data on file** whenever feasible
  - **Only collecting new data** to facilitate verification **when absolutely necessary**
    - Reasonable in light of **nature/sensitivity of PI** requested
    - **Avoid** collecting **highly sensitive PI** for 1st time
    - **Use verification-service** provider ***when no or insufficient information available*** for verification
  - Use reasonable security measures to detect fraud & prevent unauthorized access
  - **Promptly delete** newly collected PI for verification, unless needed for 24-month record-keeping
- **Accountholder authentication** procedures
  - If consumer has password-protected account, use **existing authentication** to verify consumer unless account not convenient to consumer
  - Require **reauthentication prior** to deletion or disclosure of PI
- **Unacceptable non-accountholder verification** procedures
  - As condition of submitting/fulfilling DSAR**, cannot require** consumer **to open account or use it if inaccessible**

# CCPA **DSAR** Submission & Verification

- **Risk-based verification** procedures
  - **Requests to know**: match at least **2** data points
  - **Requests for specific pieces** of PI: match at least **3** data points & obtain signed declaration under penalty of perjury
  - **Requests to delete:** match either **2 or 3** data points *based on nature/sensitivity* of PI
- **Opt-in request for children for sale of PI** - actual knowledge
  - Collects PI from children under 13: 4 consent methods for parents/guardians in draft reg
  - Collects PI from minors ages 13-17: reasonable verification of minors
  - In both case inform of right to opt-out at any time
- **Authorized agents** (register w/ CA Sec'y of State) **making DSARs on behalf of consumers**
  - Verify authorization & agent identity
  - In addition to verifying other authorized representatives (power of attorney, executor)

# CCPA **DSAR** Coordination, Timeframes, Response & Record-keeping

- **DSAR coordination**, timeframes, record-keeping & governance reporting
  - **Confirms receipt** of request to know & delete **within 10 days** with information re: process, verification & timing
  - Ensures verified DSARs properly **completed w/in 45 days** (includes verification)
    - One 45-day extension (day 1 starts w/ receipt by business) with notice & explanation
  - **Fulfillment covers** preceding **12-month timeframe** from receipt of request

- DSAR validation & consumer rights classification
  - Validate legal request
  - Classify DSAR type: right to know, data portability, deletion, opt-out

- Request execution: production, compilation, response package review & response
  - **Resource Custodians** compile & provide/delete requested PI to DSAR Coordinator

- Record retention
  - **24-month record-keeping**
  - **PI obtained for verification disposed of** after logging categories (not specific PI)
  - Cannot use these records for any other purpose
  - **Compiled data disposed of**

# CCPA **DSAR** Disclosure Fulfillment Requirements

- For each request type, specific disclosure requirements are defined covering 12-month period preceding receipt of verifiable DSAR
  - **Right to know** requests
  - **Portable data** requests
    - **In readily useable format for transmitting to another entity**
  - **Deletion** requests
    - **8 exceptions: detect security incidents, debug, legal obligations**
  - **Opt-out requests** (Do Not Sell)
    - **Suppress within 15 days of receipt & confirm with consumer**
    - **Notify 3rd parties to whom provided PI w/in 90 days that consumer has opted-out**
  - Note: **Requests to access or delete household information**
    - **If no password-protected account, provide aggregate information, or**
    - **If consumers jointly make a request & each is verified, comply with request**

# CCPA Training Program

*Driving organizational & cultural change*

- ❑ Roles-based CCPA training **needs assessment**
- ❑ **New hire & annual** awareness training
- ❑ **Organize** the following **around various roles**, e.g. management
  - ▪ **Privacy notice** training
  - ▪ Admins/receptionists & mailroom personnel (**DSAR receipt**)
  - ▪ **DSAR process** training
  - ▪ **Service provider & third party management** training
  - ▪ **Anti-discrimination** training
  - ▪ **Human Resources** training (re: employee data & security)
  - ▪ **B2B contact information** training
- ❑ **Training record retention**

# CA AG’s Rule-making Authority

- ❑ CCPA’s **specific** implementing rule-makings:
  - ✓ First: **opt-out, notice, access/portability & exception** provisions
    - *Issued with just over 2 months until CCPA becomes operative*
  - ▪ Second: **adding categories of PI** to address changes in technology, **data collection, obstacles to implementation** & privacy concerns
- ❑ **General** authority to issue rules as necessary to further Act’s purposes

# CA AG's Office re: Enforcement of CCPA

*Companies cannot be complacent in their efforts*

- **CA AG's press releases and comments -**
  - **Effective January 1, 2020, businesses must comply** with the CCPA's key requirements
- Start now – AG will **evaluate steps companies have taken** to comply before CCPA's effective date **which reflects on how seriously they view their obligations**
  - When mapping data and establishing compliance mechanisms, **document any overly burdensome technical barrier** not allowing for perfect compliance
    - Defenses relying on the technical burden or infeasibility of CCPA compliance will need to **be specific & significant**
    - **Be prepared to demonstrate compliance** by & through their policies, procedures & incident response plans, etc.

# CCPA Effective & Enforcement Dates

- **Effective Jan. 1, 2020** re: private rights of action
  - **Effective July 1, 2020 re: regulatory enforcement**
    - ***For infractions committed starting Jan. 1***
- **Extra-territorial reach** – protecting CA consumers

# Amendment Updates

*Five amendments signed into law include*

- Anti-discrimination right:
  - May charge consumer different price/rate or provide different level/quality of goods/services if difference is reasonably related to value provided to ***business*** by consumer's data
  - May offer financial incentives, including payments to consumers as compensation, for collection of PI, sale of PI, or deletion of PI
  - May also offer different price/rate/level/quality of goods/services to consumer if price/difference is directly related to value provided to ***business*** by consumer's data
- "Data brokers" that knowingly collects & sells PI to 3rd parties with whom has no direct relationship with consumer
  - Relationship can include visiting premises/website & intentionally interacting with business' online ads
  - Must register with CA AG's Office on/before Jan. 31 following each year meets broker definition & pay a registration fee
  - Unlike VT's law, data broker do not also have to offer an opt-out, but business do

# Apply CCPA with CA Residents only?

- ❑ **Consider alternative business models & web/mobile presences**, including
  - ▪ Global across the U.S.?
  - ▪ CA-only sites & offerings?

- ❑ 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*

# Prepare Early to Mitigate Class Action Risk

*Failure to undertake these efforts could lead to significant liability*

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

https://www.lexology.com/library/detail.aspx?g=e4653681-84b2-4a78-9e45-6f22884a296f

# *Data Minimization* via Privacy-by-Design

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

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

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

# Apply Lessons Learned from GDPR

- ❑ **Analyze** whether the CCPA applies to you
- ❑ **Prepare to comply** prior to Jan. 1, 2020
  - ▪ **Understand** ***compliance will take longer than you believe***, e.g. tagging & tracking data elements, fulfilling data subject rights
  - ▪ **Requires organizational, cultural & operational changes**
  - ▪ **Check-the-box compliance will fail**
- ❑ **Strong sr. leadership support & cross-functional collaboration is critical**
  - ▪ *Gain **commitment** for heavy use of enterprise-wide resources*
- ❑ **Budget appropriate funds early**

# Ponemon: Breach Cost Components & Examples

- **Detection & escalation costs: 31.1% of global cost**
  - Forensic and investigative activities
  - Assessment and audit services
  - Crisis team management
  - Communications to executive management & board of directors
- **Notification costs: 5.4%**
  - Emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen
  - Communication with regulators; determination of all regulatory requirements, engagement of outside experts
- **Post data breach response costs: 27.3%**
  - Help desk activities / Inbound communications
  - Credit report monitoring & identity protection services
  - Issuing new accounts or credit cards
  - Legal expenditures
  - Product discounts
  - Regulatory interventions (fines)
- **Lost business cost: $1.42M or 36.2% - biggest cost factor for last 5 years**
  - Cost of business disruption & revenue losses from system downtime
  - Cost of lost customers & acquiring new customers (customer turnover)
  - Reputation losses & diminished goodwill

# *General Factors Affecting avg. Breach Cost per Record*

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

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

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

**Ponemon Institute's 2019 Cost of a Data Breach Study**
507 companies (64 in U.S.) studied that experienced a breach in last year & 3,211 individuals interviewed
https://www.ibm.com/downloads/cas/ZBZLY7KL

# Raw Data Mapping SIPOC

*Ask "follow the data" questions for each unique DPLC*

| S | | I | P | O | | C |
|---|---|---|---|---|---|---|
| Data Suppliers – Data Sources | Data Resource From / Data Location | Data Inputs, Formats & How Moved / Transferred | DPLC Process Steps | Data Outputs, Formats & How Moved / Transferred | Data Resource To / Data Location | Data Customers / Endpoints |
| | | | Notice | | | |
| | | | Data Collected | | | |
| | | | Data Used / Processed / Accessed | | | |
| | | | Data Used / Processed / Accessed | | | |
| | | | Data Shared / Transferred | | | |
| | | | Data Stored / Backed-up | | | |
| | | | Data Disposed / Destruction | | | |

**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

SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Revision Date 13 Mar 2016

**Process Name:** PHI/PIIPII Processing Sample

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

Data States: At rest; in motion; at endpoints; at disposal/desruction

## Process Steps

| S | | I | P | O | | C |
|---|---|---|---|---|---|---|
| **Data Suppliers / Sources** | **Location From / Data State** | **Data Inputs** | **Data Flow Steps** | **Data Outputs** | **Location To / Data State** | **Data Customers / Endpoints** |
| Clinic / Practice | US / INTL | Signed Consent | **Notice** | Signed Consent | Locked File cabinet, Scanned to:[Shared Folder:/consents/month-Year] | Legal |
| Clinic / Practice | FedEx / UPS | sample kit, activation code, Test Requisition Form ("TRF") (name gender dob, demographics, physician info), clinical history, consent / auth | **Receive Sealed Sample Kit** | sample kit, activation code, TRF (name gender dob, demographics, physician info), clinical history, consent / auth | Receiving Area | Accessioning |
| Accessioning | Receiving Area | sample kit w/Patient name, activation code | **Open Kit: Assign barcode to sample** | sample kit w/Patient name, activation code, barcode (accessionNo) | Lab Work Bench | Lab |
| Accessioning | Lab Work Bench | TRF (name gender dob, demographics, physician info), clinical history, consent / auth, activation code | **Open Kit: Scanning paperwork with sample kit** | TRF (name gender dob, demographics, physician info), clinical history, consent / auth, activation code | [Backend Admin Tool], Shared Folder: "Sample Tracking", [Shared Folder:/consents/month-Year] | Customer Service, Billing |
| Lab | Lab Work Bench | sample w/Patient name, barcode, activation code | **Lab Processing** | sample w/Patient name, barcode, activation code; raw output | Sample into freezer; SAN storage Array | Data Processing |

# Data Mapping Benefits

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

- ❑ **Informs counsel/advisors to better advise business**
- ❑ **Informs privacy notices / customer choices** (opt-ins/outs & preferences)
- ❑ **Informs DSAR fulfillment & response process (CCPA, HIPAA, GDPR)**
- ❑ **Informs Privacy-by-Design (CCPA, GDPR)**, e.g. secondary uses, out of context
- ❑ **Informs controls evaluations & risk assessments**
- ❑ **Helps establish & maintain governance of data and resources**
- ❑ **Demonstrates governance & controls with external parties**
- ❑ **Shortens new hire learning curve**
- ❑ **Facilitates internal communications & understanding re: end-to-end DPLC**
- ❑ **Informs e-discovery & breach response pre-planning**