SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Breaking down the landmark

California Consumer Privacy Act of 2018

Information Systems Security Association (ISSA)
San Diego Chapter

Thursday, August 23
11am – 1:00pm
Fleming's Steakhouse, San Diego, CA

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

BIOs OF PRINCIPALS

Michael Cox, CIPP/US

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

Neil R Packard, CISA

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

About Us: SoCal Privacy Consultants

Educate – Assess – Operationalize - Transform

Lean, sustainable and legally defensible privacy and security programs

- Private / public customer-centric organizations in health care, Internet, technology services, financial services, etc.
- Conducts gap 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

Something to Talk About

- Introduction
- Privacy in California
- The Act
- Consumer Rights
- Enforcement
- Action Plan
- Final Notes & Summary

CA has led U.S. and often the world in codifying privacy protections

- **1972** CA Constitution amended to include the **right of privacy** among the "inalienable" rights of all people
- **2002** CA Legislature amends law defining ***"personal information" ("PI")***
- **2002 - 2017** CA legislature enacts privacy laws including:
  - CA Breach Notification Act (2002) – 1st
  - Online Privacy Protection Act (2004) – 1st
  - Privacy Rights for California Minors in the Digital World Act
  - Shine the Light Law

Previously, for many the focus has been on EU's GDPR

Now, the focus shifts to a bold new law passed by California

On January 1, 2020, organizations around the world will have to comply with CA's Consumer Privacy Act of 2018

This all started as a result of …

- **Alastair Mactaggart** and his wife having dinner with friends, including **a Google software engineer**
- He asked his friend, half-seriously**, if he should be worried about everything Google knew about him**. "I expected one of those answers you get from airline pilots about plane crashes," Mactaggart recalled recently. "You know — 'Oh, there's nothing to worry about.' "
- Instead, his friend told him there was plenty to worry about. **If people really knew what we had on them, the Google engineer said, they would flip out.**
- Mactaggart started studying the issue and **ultimately became perhaps the most important U.S. privacy activist**

https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

Citizens force legislature's hand

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

- **2017**: Californians for Consumer Privacy (CCP) started the Consumer Privacy Act ballot initiative for November election
- **2018**:
  - **May**
    - CCP submits 625K signatures for ballot measure approval
    - CCP agrees to withdraw the initiative if CA Legislature passes law addressing privacy concerns
  - **June 25**
    - CCP's initiative qualifies for the November statewide ballot
      - *Only amended by unlikely legislative supermajority, making other initiatives best but very limited option for clarifying amendments*
  - **June 28**
    - AB 375, CA Consumer Privacy Act of 2018 was **signed into law, *after only 2 days of drafting and a week of debate***
      - *Ballot initiative was withdrawn same day - deadline for such withdrawals prior to election*
      - *It was a slight compromise vs. ballot initiative, but Mactaggart held all the cards*
    - Adds to CA Civil Code: about 10,000 new words; Sections 1798.100 to 1798.198

Changes and resistance begins …

- State Senator Bill Dodd introduced **SB 1121** on August 6 as **cleanup legislation** largely intended to fix typographical errors
- A coalition of business groups, including CA Chamber of Commerce and a broad array of industry associations, wrote to state lawmakers **requesting modifications** to the definitions of "consumer" and "PI", increased operational flexibility to create and use de-identified data points, removal of data portability provision, and clarification of the non-discrimination in services provision
- However, the "**Genie is out of the bag**" – can't walk this law back
- *Expect CA State AG to provide* ***Guidance/Rules:*** ETA June 2019 & Jan 2020
- **But,** just as with GDPR don't wait – ***begin now to work towards compliance***

Who is protected?

- **Protects California residents including every individual who is:**
  - In the State for other than a temporary or transitory purpose, and
  - Domiciled in the State who is outside the State for a temporary or transitory purpose

- **Residents are Consumers** (*not Customers with relationships*) including:
  - **Employees and independent contractors**
  - **Visitors to company premises**, tenants, students, parents, children, etc.
  - **Individuals associated with commercial customers** / 3rd party relationships

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

Who must comply?

CaCPA will heavily influence data protection practices nationwide

- Every organization that collects PI for a business purpose from Californians and
  - **Sells** it, or
  - **Discloses** it
- If organization also meets **one** of three additional **criteria**:
  - Has **$25 million or more in annual gross revenue**
    - *Is not clear whether this is CA revenue or global sales*
  - Buys, receives, sells or shares PI of **more than 50,000 "consumers, households, or devices"**
  - Earns **more than half of its annual revenue selling** consumers' PI
- Given CA is 5th largest economy, behind only the U.S. as a whole, China, Japan and Germany, most global companies will want to continue to do business in CA

Who must comply?

CaCPA will heavily influence data protection practices nationwide

- *Even a **SMB** with less than $25M in revenues* could still be **subject to the Act if:**
  - **It has 50,000+ unique CA visitors annually to its website** and **makes money by** or otherwise engages in **interest-based advertising**
- **Exempts**:
  - **Non-profits (must be "for profit")**
  - **Federal privacy laws** (HIPAA, GLBA, FCRA, DPPA)
    - Although several exceptions apply only to the extent there is a conflict; meaning *where CaCPA creates new standards, courts could find there is no conflict*
- **Third-party Relationships**
  - **Data Controllers** – Do you use 3rd-party processors?
  - **Data Processors** – Do you provide services to a Controller?

CaCPA SMB Applicability

- Number of businesses
  - U.S.: **500,000+** companies
  - California: **135,000+** companies
- Vast majority of these are **small- to medium-sized businesses**
- However, this **is underestimated** as it is based on revenue and number of customers, not website visitors for example

Figures derived by an IAPP examination of the language of the law as applied to U.S. census data about American businesses.

Expands PI definition to include *almost any consumer-related data*

PI means information that **identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly**, with a particular consumer *or household* – **PI categories** include but are not limited to:

- **Usual suspects**: **unique personal identifiers** (i.e. name, SSN, postal/email address, driver's license#, passport#, etc.), **biometric identifiers** (includes sleep, health and exercise data), and **geolocation information.**
- **Commercial information**, including records of personal property and products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
- **Internet or other electronic activity information** -
  - **IP address, cookies**, beacons, pixel tags, mobile ad identifiers & similar technology, customer#, unique pseudonyms
  - **Browsing history, search history**, and info re: a consumer's interactions with a website, application or advertisement
  - **Probabilistic identifiers** that identify a particular consumer or device
  - **Other persistent identifiers** that recognize a consumer, family or device over time and across different services
- **Audio, electronic, visual, thermal, olfactory or similar information**
- **Professional or employment-related information**
- **Education information** not considered publicly available PII under the Family Educational Rights and Privacy Act (FERPA), and "characteristics of protected classifications under CA or federal law"
- **Inferences drawn** from the foregoing to create a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities & attitudes
- **Exceptions**: aggregate information not liked or reasonably linkable; publicly available info lawfully made available from gov't records used for a compatible purpose

*Given technology is increasingly capable of re-identifying data by combining various sources, be careful when pursuing data **anonymization or de-identification** strategies*

Five basic consumer rights

Extends right to privacy in CA constitution by establishing first-in-kind U.S. consumer rights over data ownership and control

Right to know	right to know, **via privacy notice & with more specifics upon request:** PI **collected**, where **sourced** from, its **use**, whether it is **sold or disclosed** & to whom; and consumer **rights** & **methods for submitting requests**
Right to (request) **deletion**	right to request **deletion of PI collected** from business servers & *service providers* with some exceptions
Right to opt-out of "sale"	right to **say "no" to sale** of PI (or for children under 16, right to no have PI sold absent parent/guardian opt-in)
Right of access & data portability	**right to access to PI in format that allows transfer** to another entity
Right to equal service & price	*right to receive **equal service & pricing, even if exercise rights**, but does permit offering financial incentives under certain circumstances*

Notice and "choice" rights

prior to or at time of PI collection

- **Right to know via privacy notice** at or at point of collection **and with more specifics upon request**
  - **Inform of**: (see slides 17 & 18 for more details)
    - **Categories & specific pieces of PI** is being **collected**
    - **Categories of sources from which PI is collected**
    - **Business purposes for collecting or selling PI**
    - **Categories of 3rd parties** with whom PI is shared; and
      - *Consumers do not have right to request names of actual 3rd party entities*
    - Consumer **rights & methods for submitting requests**
  - ***May not collect additional PI or use for additional purposes without proper notice & choice***

- **Right to opt-out of "sale"**
  - Sale means **for money or other valuable consideration** to "for-profit" **3rd party or another business** (affiliate) - *does not include service providers*
  - **After 12 months, *may request reauthorization***
  - Must add clear & conspicuous **link** on homepage titled "Do Not Sell My Personal Information" **to opt-out tool**
  - **Excludes disclosure for business purpose if** specified in privacy notice & protected by written contract with appropriate obligations & certification

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

CaCPA: What To Disclose and Where To Disclose It

WHAT MUST BE DISCLOSED		WHO MUST DISCLOSE		WHERE TO DISCLOSE	
		Collector of personal information	Seller of personal information	Online privacy notice or website's "California Rights" section	Response to consumer access request
Notice about PI processing	Categories of personal information collected about the consumer	X	X	X	X
	Categories of the sources from which the personal information was collected	X	X	X	X
	Business or commercial purpose for collecting or selling personal information	X	X	X	X
	Categories of third parties with whom the business shares personal information	X	X	X	X
	Specific pieces of personal information	X	X	X*	X
	Categories of personal information sold		X		X
	Categories of third parties to whom personal information was sold, by category or categories of personal information sold for each third party to whom personal information was sold		X		X
	Categories of personal information disclosed for a business purpose		X		X
	A list of the categories of personal information sold about consumers in the preceding 12 months or, if no sale occurred, that fact		X	X	X
	A list of categories of personal information disclosed for a business purpose in the preceding 12 months or, if no disclosure occurred, that fact		X	X	X

			WHO MUST DISCLOSE		WHERE TO DISCLOSE	
			Collector of personal information	Seller of personal information	Online privacy notice or website's "California Rights" section	Response to consumer access request
WHAT MUST BE DISCLOSED	Consumers' rights	To request access to their personal information, along with one or more designated methods for submitting such requests	X	X	X	
		To request deletion of their personal information	X	X	X	
		To opt out of the sale of their business information		X	X	
		Not to be discriminated against for exercising any of their other CaCPA rights	X	X	X	
	Financial incentives programs	Notice of any financial incentives pursuant to Section 1798.125(b)	X	X	X	
		Clear description of material terms of any financial incentive program	X	X	X	

*See discussion of: Section 1798.110(c)

Right of **Access and Data Portability**

- **Right of access/portability**
  - ***Similar to GDPR's "data portability***
  - Consumers may request access to PI and obtain it in a **"readily usable format"** that allows porting the data over to another entity "without hindrance"
  - **Upon verification** of consumer identity, business **must respond** but are not required to retain information that is obtained in a one-time transaction or to re-identify or link information that is not in identifiable form
    - *Unclear if applies to pseudonymized or de-identified data*
  - Consumers may make this request to a business **no more than twice in 12 months**

Deletion & anti-discrimination rights

- **Right to request business *to* delete any** PI collected from consumer **and** require businesses to **have its service providers delete the PI**
  - ***Similar to GDPR's "right to be forgotten"*** – not a part of ballot initiative
  - ***9 exceptions*: necessary to provide good/service** consumer requested or reasonably anticipated due to relationship with consumer; **detecting security incidents or fraud** as well as **debugging** existing systems; **enabling internal uses aligned with consumer expectations** based on relationship; complying with **legal obligations**, etc.
    - Exceptions could be **construed to be fairly broad** in nature, particularly as they related to detecting fraud, and debugging systems

- **Right to equal service and price** (nondiscrimination)
  - *Right to receive **equal service and pricing, even if consumer exercises rights** (with some exceptions) - conversely, cannot discriminate by charging different rates/services or deny goods/services to consumers who exercise rights*
    - Except if difference is reasonably related to value provided by consumer's data
  - ***Does permit offering financial incentives** reasonably related to value provided to consumer,* with notice & prior opt-in consent, for PI collection, sale & deletion
    - *Could pay for PI use or privilege of remaining anonymous*

Operationalizing consumer rights

For **consumer-specific requests**, Act requires:

- Providing 2 or more designated methods for submitting requests, including at a min., **a toll-free PH#,** & if business has a website, a **Web address**
- Verifying (authenticating) requesting consumer without undue hindrance
- Request be made **in writing** and information should be provided:
  - **Free of charge**
  - **In** readily useable (portable) **format allowing data to be transferred** to another entity ***without hindrance***
  - **Within 45 days** of request
    - time 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
- Develop and implement rights **operational processes**
  - **When electing not to substantively respond, inform** of reasons for not taking action & any rights to appeal, recognizing desire to avoid an action
    - *Can charge a fee or refuse to respond, if* manifestly unfound or excessive, particularly if repetitive in character
- **Requires training** of appropriate staff responsible for handling:
  - Consumer **inquiries** about rights & privacy practices
  - **Rights requests**

How enforced?

*Exposes businesses to potentially large **civil penalties***

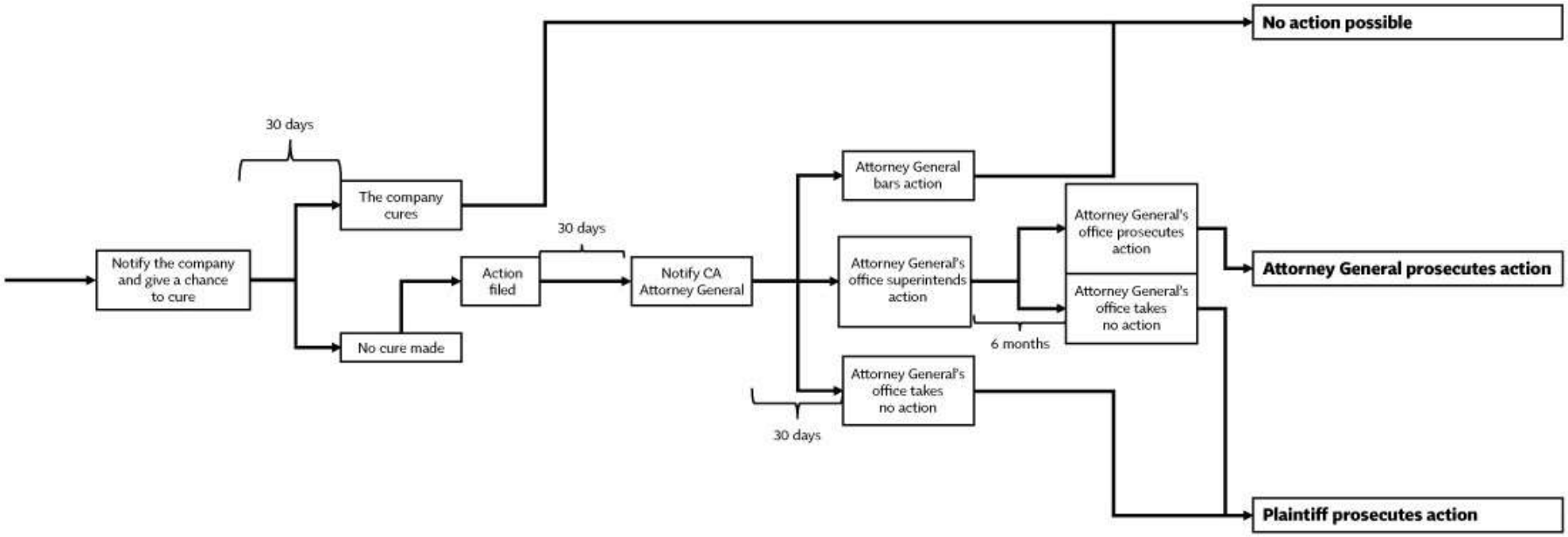
- Enforced by **CA State Attorney General** (Facebook happy this was not in previously place)
  - Businesses failing to cure within **30-day cure period** face a penalty of:
    - **Up to $2,500 for each violation** (likely per consumer), or
    - **Up to $7,500 for each intentional violation** (willful unfair competition violation)
  - **20% of such penalties** collected by CA **to fund enforcement**
- **AG** is the rule-making authority
  - Specific implementing rules:
    - **June 28, 2019**: opt-out, notice, access/portability, & exception provisions
    - **January 1, 2020**: adding categories of PI to address changes in technology, data collection, obstacles to implementation, and privacy concerns
  - General authority to issue rules as necessary to further the Act's purposes

Consumer right to sue

Exposes businesses to potentially ***large statutory damages***

- **Individuals can only bring a civil action if**: (can be aggregated into class action)
  - Their non-encrypted/non-redacted **PI is compromised in a data breach** (“*subject to unauthorized access and exfiltration, theft or disclosure*”) **due to a failure to** implement and **maintain reasonable security procedures;**
    - *Keep in mind the* ***definition of breached PI is narrower*** *than CaCPA’s PI definition*
  - **Business has not cured violation** and provided “express written statement” that violation has been cured and “no further violations (will) occur” within **30-day cure period**; and
    - ***Can sue if*** *business* ***continues to violate*** *CaCPA in breach of its written statement*
  - **Provides additional 30-day pre-suit written notice** identifying specific statutory violations **to State AG** who can notify consumer of intent to prosecute or to “not proceed” with the action, or not act within 30 days allowing consumer to proceed
    - If AG does not act within 30 days of notice or proceed with action within 6 months of informing plaintiff of intention to prosecute, plaintiff can continue action unimpeded
- **Civil penalties: greater of statutory damages of $100-$750 or actual damages** per incident

Right to Sue Process



https://media.iapp.org/2018/08/21105110/Liability-flowchart.jpg

Apply CaCPA with CA residents only?

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

- However, also consider:
  - **Impact on customer relations** of differentiating service to residents of CA and other states
  - **Legal implications of voluntarily representing and applying CA law across other states**
    - Keep in mind that other states following CA's lead may impose differing privacy laws

Action Plan

For some, GDPR provides a boost towards compliance

1. **Prepare and maintain data maps, inventories or other records** of all PI pertaining to CA residents, households and devices, as well as data sources, storage locations, usage and recipients, and based on this information:
   a. **Inventory and maintain all 3rd party service providers/vendors and update agreements** re: compliance with CaCPA
   b. **Update privacy notices** to add newly required disclosures about consumer rights **& update at least annually**
   c. **Update privacy policies re: data access, deletion, and portability rights fulfillment and other CaCPA obligations**
   d. **Train workforce members**
   e. **Track data streams to identify CA residents and track/flag PI: when & how collected in last 12 months; with whom shared; where located and how long; and to honor opt-in/out choices**

2. **Make available designated methods for submitting data access requests**, including, at a min., a toll-free phone#

3. **Provide clear, conspicuous "Do Not Sell My Personal Information" link** on business' Internet homepage, that directs users to a web page enabling them, or someone they authorize, to opt out of the sale of resident's PI

4. **Fund and implement new systems and processes** to comply with the new requirements, including to:
   a. **Verify identity and authorization of persons who make requests** for data access, deletion or portability
   b. **Respond to rights requests** for data access, deletion and portability **within 45 days**
   c. **Avoid requesting opt-in consent for 12 months after a CA resident opts out**

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

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

https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/

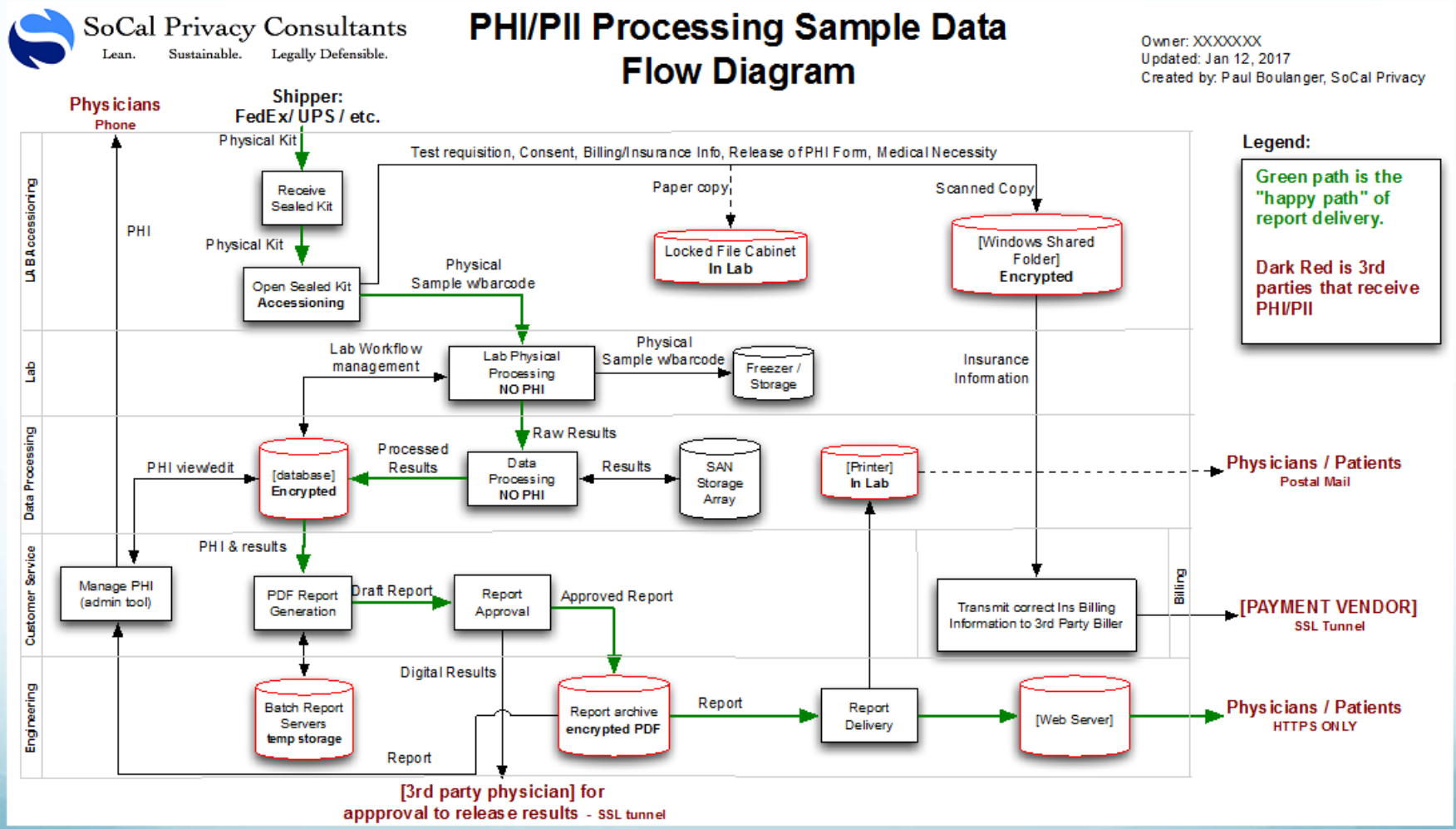
Data Mapping

- **Data Lifecycle**
  - **Develop data flow, inventory, and resource map *for every data set***
    - e.g., business units/channels/subsidiaries, Human Resources, mobile apps, websites, and physical stores generally have different DPLCs and thus require separate data mapping sessions and maps

- Should be **formalized, repeatable process** composed of:
  - **Identifying / inventorying** what personal data is collected, used, shared, stored and disposed
  - **Classifying** the highest level of **data sensitivity** (based on the data inventory) in each resource
  - Identifying what data is transferred to externally
  - Inventorying all resources
  - **Assigning a resource owner and custodian** to each resource for governance purposes (and separation of duties)

Sample Data Flow Diagram

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



Data Mapping Benefits

Most entities have *inadequate* understanding of *end-to-end* Data Lifecycle processes

- **Informs counsel / advisors to better advise business / clients**
- **Informs controls evaluations & risk assessments prior to kick-off**
- **Informs Privacy-by-Design / PIAs**
- **Informs privacy notices & customer choices** (opt-ins /outs)
- **Informs of needed security** (discover & protect unknowns)
- **Demonstrates governance & helps maintain governance**
- **Shortens new hire learning curve**
- **Facilitates organizational understanding / communications**
- **GDPR: Helps identify data collected & all DPLC processes to inventory, analyze & document re: lawful processing purposes**

Governance and maturity tips

This is not a check-the-box compliance drill

- **Establish budget** for foreseeable 2019 costs
- **Integrate Privacy/Security-by-Design** with engineering/development
- **Integrate new required operational practices into existing policies/SOPs**
- **Train all appropriate staff**
- **Ensure ownership, governance and roles and responsibilities** are well defined and communicated for sustainability (NIST's repeatability)
  - Beware of "**conflicts of interests**" and "**separation of duties**"
- **Establish monitoring/oversight of key activities** for repeatability
  - *Review, logging, tracking, reporting and follow-up*
- **Implement periodic self-assessment or audit** to evaluate compliance gaps and ensure sustainability and maturity
- **Document** decision-making, monitoring, evaluations/assessments in a compliance repository demonstrate accountability
  - Ensure **investigational preparedness** to timely and comprehensively respond
- **Consulting and Legal** - *seek SME advice and support*

Modify data monetization business models

Brace for additional penalties and liquidated damages

Final Notes

- Congress may act and consider passing omnibus federal privacy law that harmonizes or preempts diverging and patchwork state laws
  - Silicon Valley tech giants now appear to be supportive of this
  - However, substantively watering down CaCPA should not be the goal
- Given options, instead of a take it or leave it approach, we as consumers should thoughtfully consider the value of free services (where we are the product) vs. the need for more regulation which will adversely impact consumer taxes and cost of goods and services
- CA Legislature to make technical fixes and perhaps substantive changes
- Constitutional and pre-emptive challenges
- It is about finding "**the right balance**"

Summary

- **California is on the *bleeding edge* of Privacy in U.S.**
- **CaCPA furthers Californians' right to privacy**
  - Provides consumers an effective way to control their PI
  - Right to know, delete, opt-out, access/portability and anti-discrimination
  - Effective January 1, 2020
- **Don't Wait**
  - 16 months is not a lot of time as anyone who has been working on GDPR compliance knows full well

Questions?

Contact

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

Neil R Packard, CISA
npackard@socalprivacy.com
619.208.2529

www.socalprivacy.com

Appendix

Supplemental Analysis
About Us

General Analysis Points

- Drafters did not address any overlap or inconsistencies between new law and any of California's existing privacy laws
- Instead, the new law prescribes that in case of any conflicts with California laws, the law that affords the greatest privacy protections shall control
- Notably it instructs courts that the new law "shall be liberally construed to effectuate its purposes“
- CA has moved from sector- and harm-specific privacy legislation to a much broader and comprehensive privacy regime
- Consequently, companies, privacy officers, lawyers and others will have to deal with an even more complex and fragmented privacy law landscape in CA, and therefore in the U.S. and the world

https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/

Lean, sustainable and legally defensible

- ***Lean* – *strength of controls based on data sensitivity and risk***
- ***Sustainable* –** *operationalize through* ***governance and clear roles, responsibilities & practices*** *(NIST's repeatable RM Tier)*
- ***Legally defensible* –** *able to defend actions* ***to a regulator and plaintiff judge or jury***

Why SoCal Privacy?

Key aspects of who we are at the core

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

- ***We're not recent college graduates using a checklist – we're experienced professionals***
  - *Michael has testified before three FTC lawyers for two hours on behalf of a client*
  - *Michael served as part-time Chief Privacy Officer of an international company for 8 years*
  - *Neil has audit and e-discovery experience and understands FTC expectations having worked there*
- ***Understand client's business and how to operationalize practices/processes***
  - *Conducting data mapping first allows us to get our arms around your business to better advise you during the gap and risk assessment*
  - *Michael's previous operations executive experience allows him to provide practical advice on how to operationalize practices as repeatable processes*
- ***Understand IT technical systems and controls***
  - *Neil's experience allows him to offer deep dive technical advice*

SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Certified, experienced privacy and security professionals arm you with the knowledge, tools and confidence to build and establish a practical, sustainable, and legally defensible Privacy and Security Program with our 2-phased process:

Phase 1 – Gap Assessment

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

Phase 2 - Implementation

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

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

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

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