The California Consumer Privacy Act, Part 2
Data Privacy Management

May 2019

This SecureTheVillage Webinar brought to you by …

PEPPERDINE | GRAZIADIO BUSINESS SCHOOL

CyRP

CITADEL
INFORMATION GROUP, INC.

CybersecureLA 2019
Cybersecurity is a Team Sport

… a joint presentation of SecureTheVillage and Pepperdine Graziadio Business School

October 17, 2019 … Mark Your Calendars

The California Consumer Privacy Act Data Privacy Management

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guests
  - *Ilanna Bavli, Esq., Eleven/11 Counsel & Strategy, SecureTheVillage Board*
  - *David Grazer, CIPP-US, SecureTheVillage Leadership Council*

Topics and Outline

- CCPA Privacy Overview
- Data Privacy Management Objectives
- The Data Inventory: Getting Started
- Illustration: Data Inventory Components
- Developing the Data Inventory
- Documenting the Data Inventory
- Use of Data Inventory Tools
- Key Challenges

ResourceKit:

The California Consumer Privacy Act (CCPA), Part 1, April 2019

Information Classification & Control Webinar, August 2018

CCPA: California Law Codifies Consumer Privacy Rights

- Commencing 1/1/2020, consumers have
  - **Right of Disclosure: To request the categories and pieces of information collected, sold, or disclosed about the consumer going back 12 months**
  - **Right of Deletion: To have certain information deleted, both from the business and any service providers with which the business shared the information.**
  - **Right to Opt-Out: To opt out of the sale of their information**
    - **Explicit opt-in under the age of 16 must explicitly opt in to any such sales**
  - Right to Be Compensated in Event of Data Breach:
    - Private Right of Action
    - Statutory Damages
    - Definition of PII
- Applies to a for-profit business that collects consumers' personal information that does business in California and that:
  - Has annual gross revenues greater than $25M, or
  - Obtains personal information of 50,000 or more consumers, households or devices annually
  - Derives 50% or more of its annual revenues selling the personal information of consumers
- **Includes exceptions for Other Regulatory Privacy, e.g., HIPAA**
- Requires new privacy disclosures
- Reasonable security procedures and practices appropriate to the nature of the information being protected qualifies compensation right

Data Privacy Management Objectives

- Business Must Be Prepared for Request to Disclose or Delete
- Know Your Information
  - What it is
  - Where it is
  - Who Manages It
  - Why You Have It
  - How Long You Keep It
  - To Whom You Provide Access
  - How You Secure/Delete It

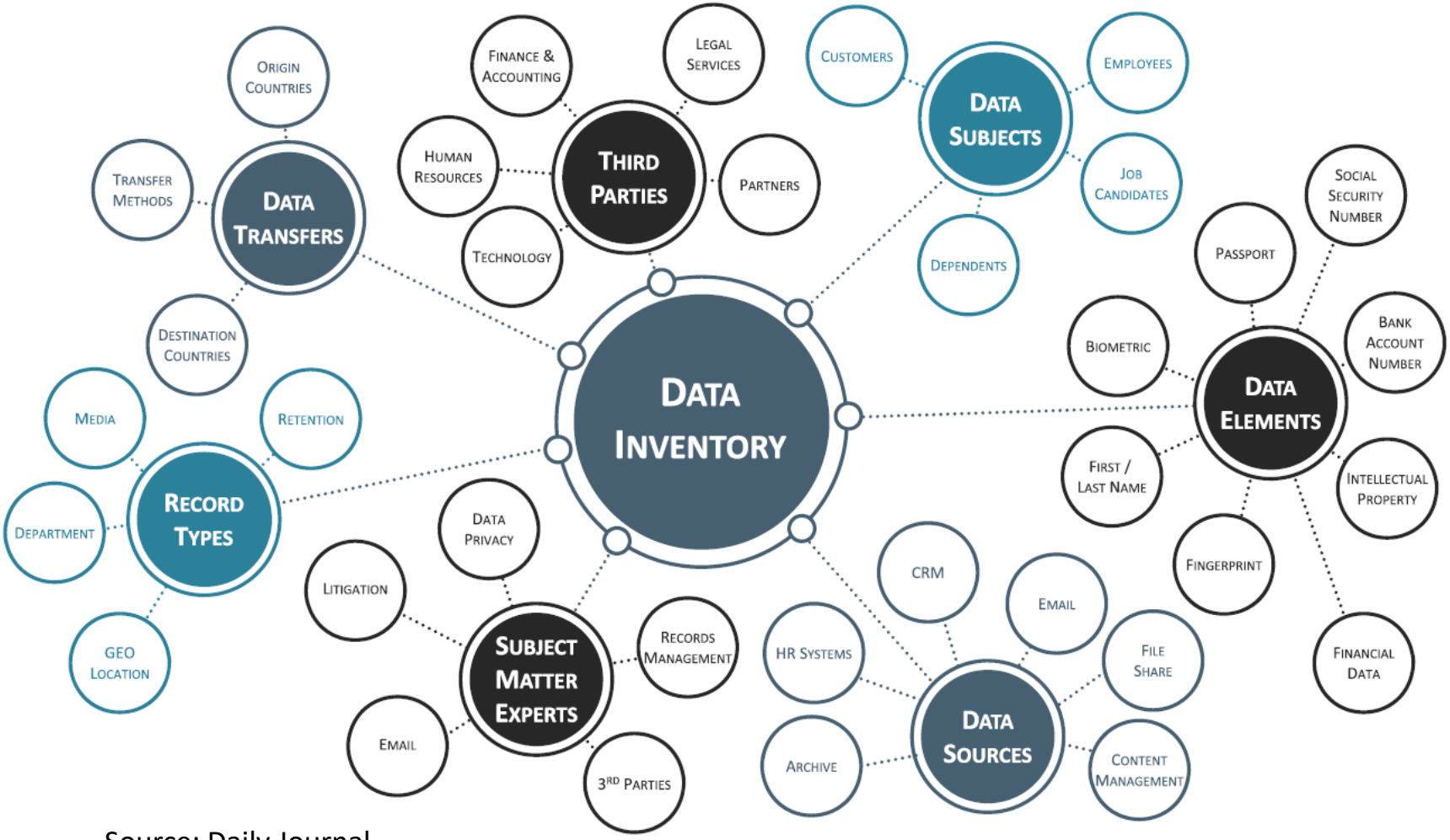
Understanding how the company collects, processes, transmits and stores data – as well as how it's used and who uses it – is the foundation of a data privacy program and the key to complying with the Act and most other privacy regulations.

Robert Braun, JMBM and STV Leadership Council

The Data Inventory: Getting Started on the Information Life-Cycle

- What Data Might You Have; General Categories
  - Name, Addresses, SSN
  - Credit Cards
  - Health Information
  - Email Addresses
  - Digital Identities
  - Internet Activities
  - Consumer history
  - Etc
- Information Gathering Questions
  - What data do we actually gather?
  - What systems / services use the data?
  - How long do we keep the data?
  - With whom do we share data?
  - How is this data protected?

Illustration: Data Inventory Components



Source: Daily Journal

Developing the Data Inventory

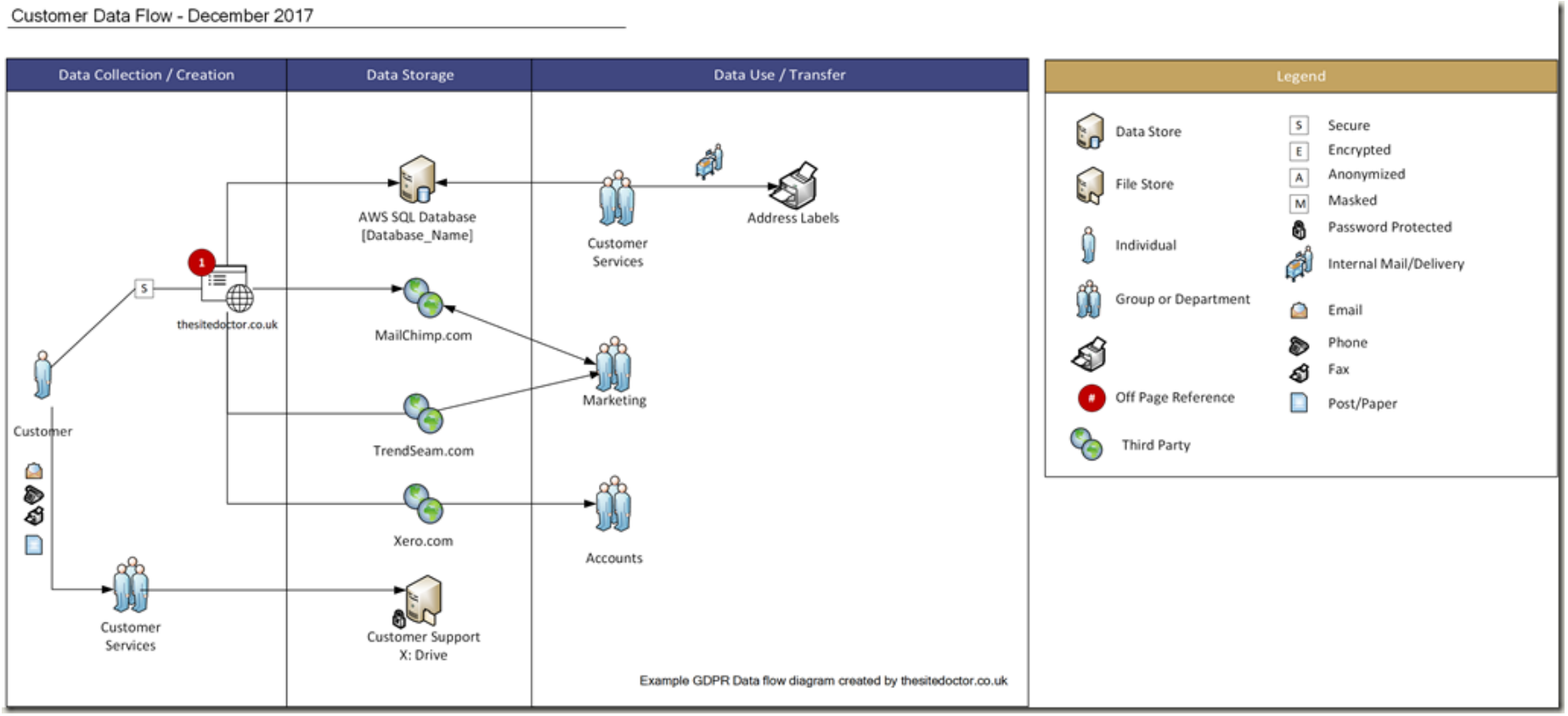
- Leadership-driven initiative
- Cross-Functional & Collaborative
  - Involved Departments
  - IT
  - Infosec
  - Law
- Break Down Silos
- Interview Subject Matter Experts at All Levels
  - Interactive process
  - Follow up
  - Dig deep
- Develop Procedures
- Update 3rd-Party Agreements

Documenting the Data Inventory

Information Category	Information Belongs To	Information Description	Owning Department	How / Where / When Collected?	Dep'ts Transferred To	3rd-Parties Transferred To	Transfer Nature (Sale, Provision of Service, ...)	Information Retention Period
Marketing	Customer	IP Address of website vistor	Marketing	During web visit	None	Acme Marketing	provision	12 months
PII	Customer	Customer Name/Address	Marketing	During web visit; via email; via phone	Finance; Operations	Equifax	Sale	unknown
PII	Customer	Customer email	Marketing	Online; In store	Sales; Operations	Mailchimp	Provision	While "live"
Financial	Customer	Credit Card Info	Sales	In store; Online	Finance	Equifax	Sale	unknown
Financial	Contractor	Bank account number	Finance	Operations, during onboarding	None	Bill.com	Provision	During engagement + 12 months

- Spreadsheets
- Network Maps
- Visio Diagrams
- Data-Flow Diagrams
- Reports / Narratives

Data Mapping: An Illustration



Use of Data Inventory Tools

- Compliance Tools
  - Spreadsheets
  - Program Management
  - Data Discovery
  - Special Purpose Tools
    - Inventory
    - Deletion
- Data classification tools built into AWS, SQL, etc.
- Beware: Tool Incompatibility with Existing Tools
- Beware: Tool Bloat
- Beware: Leaving Out Human Piece
- See *IAPP Privacy Tech Vendor Report (iapp.org)*

Key Data Privacy Management Challenges

- Systemic Challenges
  - Leadership
  - Cross-Functional Communication
  - Shadow IT
  - Legal Interpretation / Risk-Tolerance
  - Changing Compliance Requirements
  - Treating CCPA in Isolation from Other Security & Privacy Requirements
- Human Challenges
  - Failure to ask the right questions
  - Failure to Be Transparent
  - Fear of Sharing Information
  - Fear of Being Wrong
  - Fear of Criticism
  - Not knowing “why”

Next Webinar: June 6, CCPA, Part 3 Minimum Reasonable Security Practices

- CCPA, Part 3: Minimum Reasonable Security Practices
  - *If you're not doing these, then your practices are not reasonable*

The California Consumer Privacy Act (CCPA) private right of action establishes statutory damages of between $100 and $750 per incident for consumers whose personal information has been compromised by a breach of personal information resulting from the business' "violation of the *duty to implement reasonable security procedures and practices* appropriate to the nature of the information to protect the personal information."

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives understand how to turn their organization into Cyber Guardians and create a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Minimum Set of Reasonable Security Practices: A set of information security management practices so basic as to be necessary for a claim that one's information security practices and procedures are reasonable. *Under development in support of CCPA.*

Community-Based Programs: Train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

For More Information …

Stan Stahl, SecureTheVillage & Citadel Information Group
Stan@SecureTheVillage.org
323-428-0441

Ilanna Bavli, Eleven/11 Counsel & Strategy
ibavli@eleven11counsel.com
(323) 688-0111

David Grazer
grazerda@gmail.com
(949) 632-8920

CybersecureLA 2019
Cybersecurity is a Team Sport

… a joint presentation of SecureTheVillage and Pepperdine Graziadio Business School

October 17, 2019 … Mark Your Calendars

FREE Citadel *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*
https://Citadel-Information.com

Follow SecureTheVillage on LinkedIn: https://www.linkedin.com/company/secure-the-village
Follow Citadel on LinkedIn: https://www.linkedin.com/company/citadel-information-group

For Marketing / Sponsorship Opportunities
Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject
Visit us at https://securethevillage.org/sponsorship-opportunities/

Thank You

The California Consumer Privacy Act, Part 2
Data Privacy Management

May 2019