DrinkerBiddle®

California Consumer Privacy Act Overview

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") takes effect on January 1, 2020.

KEY DEFINITIONS

Despite its name, the CCPA applies to a broader class of individuals than colloquial understandings of "consumers." The term "consumer" is defined under the Act, in relevant part, as "a natural person who is a California resident." Thus, customers, employees, business contacts, and others are protected individuals under the Act.

"Personal Information" is broadly defined under the CCPA and includes a number of enumerated categories of personal information. In general, information that can be linked to a person, device, or browser will be considered "personal information."

KEY REQUIREMENTS

The CCPA empowers CA residents with the following six data privacy rights:

1. To be provided with information on what personal information is collected about them and the purposes for which that personal information is used.
2. To be provided with information on what personal information is sold or disclosed for a business purpose and to whom.
3. To opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information).
4. To request the deletion of their personal information.
5. Not to be subject to discrimination for exercising any of the above rights, including being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services.
6. To seek statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of a business' violation of its duty to implement and maintain reasonable security procedures.

The CCPA also requires that a business must in its online privacy policy, or in a California-specific privacy policy posted on its website, describe CA residents' rights to request information and list the categories of CA residents' personal information it has in the prior 12 months (i) collected, (ii) sold, and (iii) disclosed for business operational purposes.

In addition to describing the right to opt-out in its online privacy policy or California-specific privacy policy, a business must include a "clear and conspicuous" link on its homepage to a web page where individuals can exercise their opt out rights. The link must be titled "Do Not Sell My Personal Information" and must link to a page with the same title.

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON

Promotional materials 01242019. One Logan Square, Ste. 2000, Philadelphia, PA 19103-6996 (215) 988-2700 *office* (215) 988-2757 *fax*
Dorothy E. Bolinsky and Andrew B. Joseph, Partners in Charge of the Princeton and Florham Park, N.J., offices, respectively.

DATA MAPPING SERVICES

A DATA-CENTRIC VIEW OF THE WORLD

IT departments have long maintained inventories of their organization's technology infrastructure – essentially, a map of systems, applications, servers, networks, and other components. While this map is necessary for IT management, it does not support the data-centric viewpoint necessary to support critical information governance activities like information protection, e-discovery, data analytics, and retention. The realities of competing in a data-driven world and the proliferation of national and global legal and regulatory requirements make this data-centric approach more important than ever.

A TEMPLATE FOR PROTECTING AND LEVERAGING DATA

A comprehensive data map contains "data about data" that enables organizations to govern and leverage their own information assets. Creating a data map is more challenging than ever, as the generational shift in enterprise IT currently underway is radically changing not only the way employees create data, but where and how that data is stored. Organizations are rapidly adopting mobile and cloud-based tools that create **more diverse forms of data** than ever before; **stored in more places** than ever before; under **more complex management and control** arrangements than ever before. This evolution makes the creation and maintenance of the enterprise data map more important than ever.

Although the specific drivers for each organization are different and evolve over time, three critical data mapping needs include:

I. **Electronic Discovery.** At the outset of litigation, parties are under a duty to identify all potentially responsive sources of data and to take reasonable steps to preserve and produce this information. This requirement is difficult to meet without a good data map, and the consequences of failure include fines, sanctions, and negative case outcomes.

II. **Privacy Requirements.** Organizations quite simply cannot comply with privacy laws like the EU General Data Protection Regulation (GDPR) and the newly enacted California Consumer Privacy Act that require organizations to have a comprehensive, accurate, and up-to-date view of the private data they hold, and to implement controls to adequately protect and govern that information. The consequences of failure in this area can be extreme – in the case of GDPR, up to 20 million euros or 4% of annual revenue, whichever is higher – to say nothing of the reputational costs.

III. **Cybersecurity.** To properly protect valuable information assets, organizations must have a comprehensive understanding of the value of their data, its logical and physical location, access control requirements, and a myriad of other critical data points that drive where and how cybersecurity resources are deployed. A data map is essential to cybersecurity.

TAKING ACTION: DATA MAPPING SERVICES

Tritura offers a full range of services related to data maps, from the ground-up creation of a new enterprise data map to providing high-level current state assessments. We tailor our approach to the needs, size, and complexity of our clients, while offering:

- **Insight.** Comprehensive insight into all sources of data within an organization through the use of analytical software and custodian interviews.
- **Analysis and Reporting.** A sophisticated data map inventory in client-preferred formats, using data visualization techniques, spreadsheets, and other narrative formats.
- **Compliance Implementation. A** full range of privacy and cybersecurity compliance services designed to help clients leverage their data map investment by achieving compliance.
- **Data Remediation.** A suite of services enabling clients to fully remediate data based on insights gained through the data mapping process.

CONTACT

Contact our team to discuss your data mapping questions and needs with our experts.

Bennett B. Borden
Chair
(202) 230-5654
Bennett.Borden@dbr.com

Jay Brudz
Chair
(202) 230-5195
Jay.Brudz@dbr.com

DrinkerBiddle

Hand Me the Map, Please

The Critical Role of Data Mapping in CCPA Readiness and Compliance

Wednesday April 3, 2019 1:00 PM EDT

Jay Brudz and Barclay T. Blair

Presenters

Jay Brudz

Partner

Drinker Biddle

Barclay T. Blair

Founder and Executive Director

Information Governance Initiative

Status of CCPA

- Operative January 1, 2020 (reminder: GDPR became effective May 25, 2018)
- California's Attorney General has up to six months (July 2, 2020) after that to publish implementing regulations.
  - Regulations may: change what is considered personal information; establish exceptions required to comply with federal or state law; create procedures for how entities handle consumer opt-out requests, etc.
  - Draft regulations expected Fall 2019
- The AG may not bring an enforcement action until six months after the rules are published or July 1, 2020-whichever is sooner

Despite What You May Have Heard, it is Not:

Who is Affected by CCPA

- Any entity doing business in the State of California with at least one of these characteristics:
  - Annual gross revenue over $25M
  - In the business of buying or selling the personal information of 50K or more consumers, households, or devices
  - Derives at least half their revenue form selling personal information

CCPA Key Provisions and Definitions

- **Consumer**: a natural person who is a California resident.” Thus, customers, employees, business contacts, and others are protected individuals under the Act.

- **Personal Information**: information that can be linked to a person, device, or browser will be considered “personal information.”

1. To be provided with information on what personal information is collected about them and the purposes for which that personal information is used.
2. To be provided with information on what personal information is sold or disclosed for a business purpose and to whom.
3. To opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information).
4. To request the deletion of their personal information.
5. Not to be subject to discrimination for exercising any of the above rights, including being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services.
6. To seek statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of a business’ violation of its duty to implement and maintain reasonable security procedures.

Why Do We Need a Map? Supporting 6 Key CCPA Requirements

1. To provide consumers with information on what personal information is collected about them and the purposes for which that personal information is used.
2. To provide consumers with information on what personal information is sold or disclosed for a business purpose and to whom.
3. As a foundation for a process enabling consumers to opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information).
4. To respond effectively to consumers requesting the deletion of their personal information.
5. To ensure that consumers are not to be subject to discrimination for exercising any of the above rights, including being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services.
6. To prevent and defend against consumers seeking statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of violating our duty to implement and maintain reasonable security procedures.

The Map

Stoke Gifford
Parkway
Bradley Stoke
Winterbourne
Ring road
Kingswood
A 4174
(M 32, M 4)
Bristol
(M 32)
Yate (A 432)

CCPA Data Mapping

- CCPA (unlike e.g., GDPR) does not explicitly contain a data mapping requirement
- However, it is clear that it will be difficult - if not impossible - to comply with CCPA without one
- It is unlikely that your existing data maps (or system inventories, privacy registers, IT asset logs, e-discovery “litigation likely” maps, records retention inventories, etc.) will serve this purpose well (although of these are useful sources of insight).
- A key difference in focus for CCPA vs. other drivers of data maps is a focus **on data flows, i.e., a relationship map**

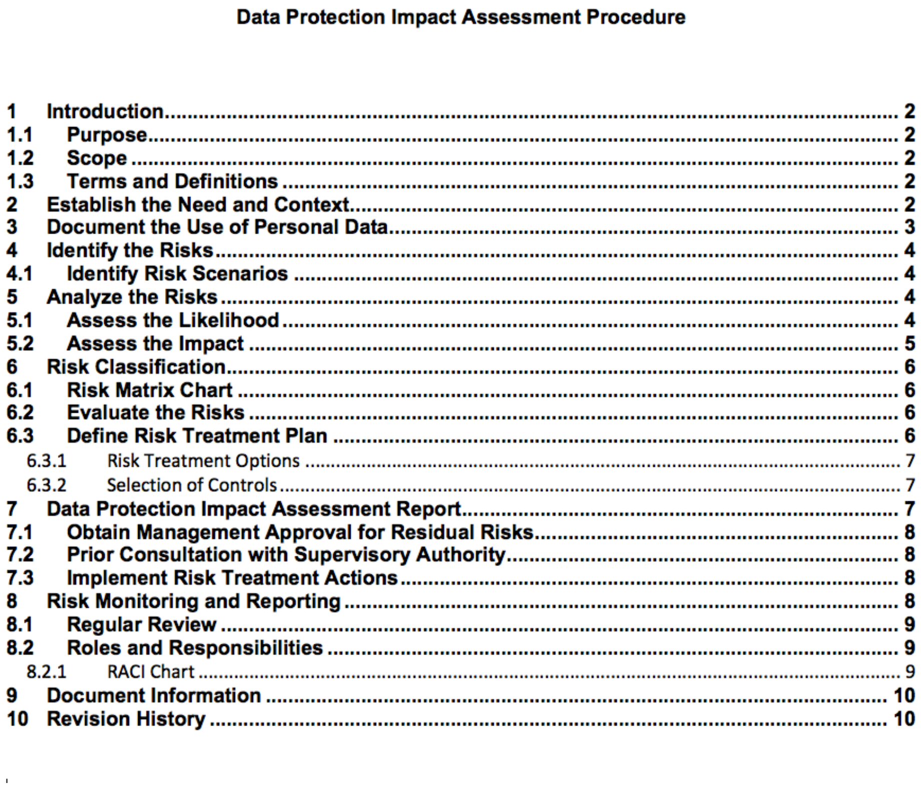
Can You Rely on Prior Data Mapping Work?

- Any of your baseline methodologies and systems used for data mapping – regardless of the reason - will have some utility.
- However, there are some key differences and unique challenges to be aware of (and likely will be more when the implementing regulations are published Fall 2019)

- For Example
  - CCPA contains the concept of a “household” whereas GDPR does not.
  - CCPA’s definition of personal information is broader than most prior definitions in US law.
  - CCPA exclused PI that is already governed by privacy law (e.g., GLB, HIPAA), so those exclusions must be catalogued and tailored to CCPA.

Leveraging GDPR Compliance Efforts

- Data Privacy Impact Assessments
- Privacy Information Data Inventory
- Supplier Assessment Procedures
- Private Data Legitimate Interest Procedures
- Procedures for International Transfers of Personal Data
- Personal Data Collection and Processing Assessments
- Supplier Data Process Agreements
- Vendor Security Evaluation Procedure
- Process Contract Review Procedure
- Data Flow Registry
- Personal Data Breach Register
- Security Incident Response Plan



Data Protection Impact Assessment Procedure

Entries on the Data Map

- **The Country (The Organization).** First and foremost any map define its borders. Your data map border is your organization, but you may need to be more precise - i.e., what parts of the organization (e.g., by geography, line of business, function etc.) does your map include?
- **States/Provinces (Departments)**. Your country is organized into several states. Your states are the departments, business units, and other groupings of people and processes that engage in identifiable and distinct activities with PI.
- **Cities (Information Systems).** There are cities across your country that your states rely upon to collect, access, process, and transfer PI. These may be shared by multiple States and thus be located in/managed by your Capital City (e.g., messaging, collaboration), or may only be controlled or used by only a single state (e.g., financial systems).
- **Local Government (Responsible Parties)**. At the state, city, and other levels of your country, you have delegated authority for how the cities are run, how natural resources are exploited and transported. The people in charge across the country must be noted on your map.
- **Roads and Rivers (Data Flows)**. Your natural resources flow across your country using a complex and ever-changing network of transportation pathways and methods. These must be on your map.
- **Natural Resources (Data).** Your country buys, sells, stores, transports, and processes natural resources, i.e., your data across the country. Your map has to record where those resources originate from and where they are stored. Not all natural resources have the same value or risk.
- **Uranium (Private Data)**. Your country also buys, sells, processes, stores, and transports a particular kind of natural resource that is very valuable and a critical component of national growth and prosperity - but one that has risks, must be handled properly, and is subject to multiple restrictions and requirements that must be followed.
- **International Partners**. Your country does business with multiple entities outside your borders. Sometimes you sell them natural resources, including uranium, sometimes you buy it, and sometimes you share it.

How Else Can You Use Your Data Map?

- Information Governance
- E-Discovery
- Information Security
- Breach notification
  - Contractual obligations
  - Consumer notification

Where do we start?

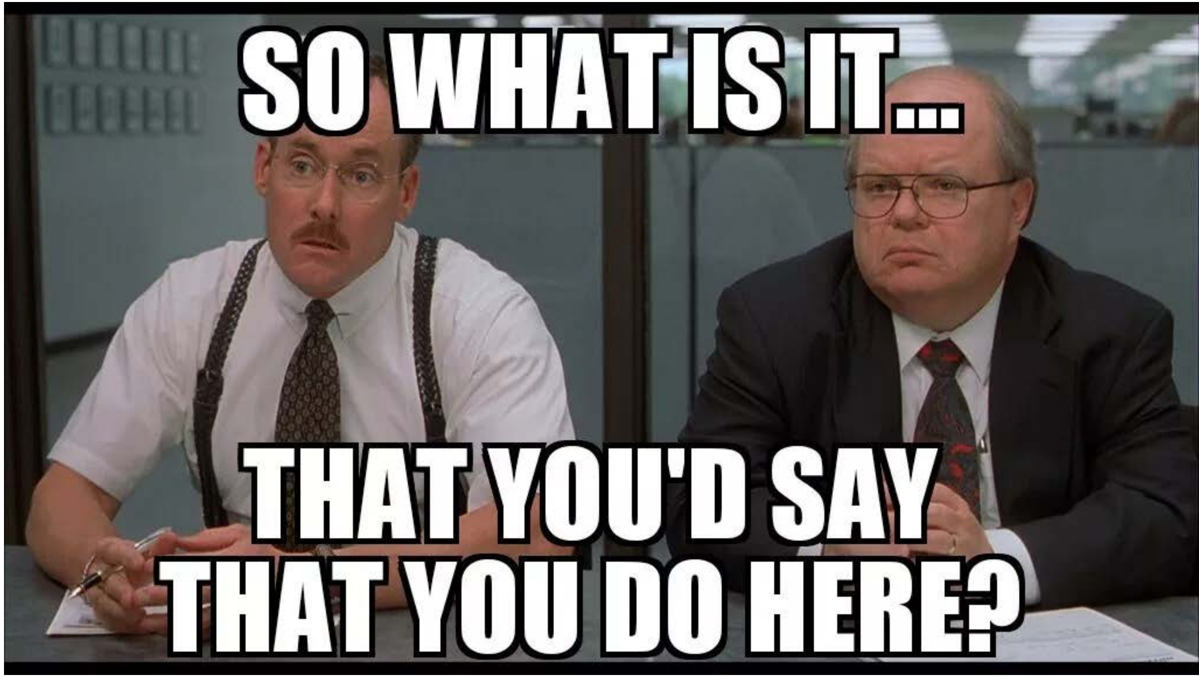
- Gather documents
- Org Chart
- Vendor contracts
- Key Personnel
- Pre-kickoff with core team

Kickoff

- Change Management Principles
- Executive Champion
- Stakeholders
- Business
- IT
- IG
- Legal

Interviews

- Group by business / function
- Include IT liaison if possible
- Choose seniority carefully



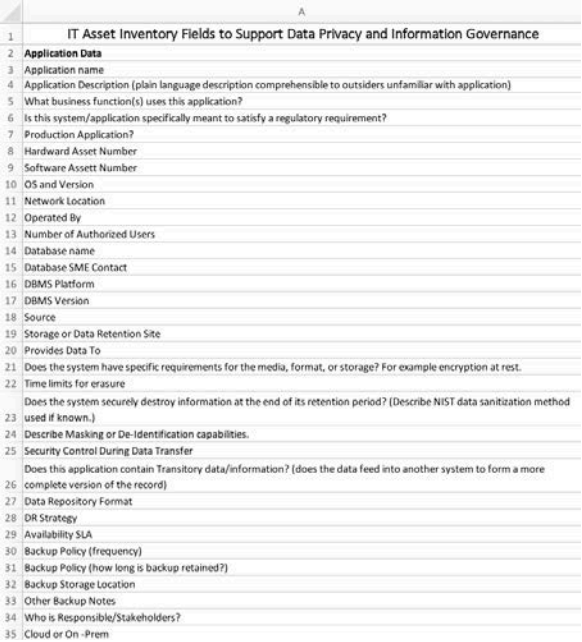
Interview Methodology

- Inverted Pyramid
- Interlocutor and Amanuensis
- Be Fearless
- Allow buffer time between interviews

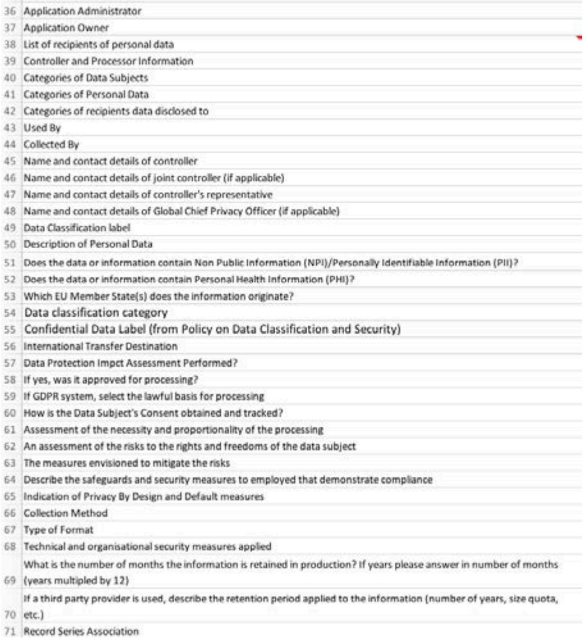
Iterate

- Pay attention to keywords
  - System names
  - Acronyms
  - Names of documents
  - Things That Sound Capitalized!
- Rinse, repeat

End Product: Can Take Various Forms, e.g.



	A
1	IT Asset Inventory Fields to Support Data Privacy and Information Governance
2	**Application Data**
3	Application name
4	Application Description (plain language description comprehensible to outsiders unfamiliar with application)
5	What business function(s) uses this application?
6	Is this system/application specifically meant to satisfy a regulatory requirement?
7	Production Application?
8	Hardward Asset Number
9	Software Assett Number
10	OS and Version
11	Network Location
12	Operated By
13	Number of Authorized Users
14	Database name
15	Database SME Contact
16	DBMS Platform
17	DBMS Version
18	Source
19	Storage or Data Retention Site
20	Provides Data To
21	Does the system have specific requirements for the media, format, or storage? For example encryption at rest.
22	Time limits for erasure
23	Does the system securely destroy information at the end of its retention period? (Describe NIST data sanitization method used if known.)
24	Describe Masking or De-Identification capabilities.
25	Security Control During Data Transfer
26	Does this application contain Transitory data/information? (does the data feed into another system to form a more complete version of the record)
27	Data Repository Format
28	DR Strategy
29	Availability SLA
30	Backup Policy (frequency)
31	Backup Policy (how long is backup retained?)
32	Backup Storage Location
33	Other Backup Notes
34	Who is Responsible/Stakeholders?
35	Cloud or On -Prem



36	Application Administrator
37	Application Owner
38	List of recipients of personal data
39	Controller and Processor Information
40	Categories of Data Subjects
41	Categories of Personal Data
42	Categories of recipients data disclosed to
43	Used By
44	Collected By
45	Name and contact details of controller
46	Name and contact details of joint controller (if applicable)
47	Name and contact details of controller's representative
48	Name and contact details of Global Chief Privacy Officer (if applicable)
49	Data Classification label
50	Description of Personal Data
51	Does the data or information contain Non Public Information (NPI)/Personally Identifiable Information (PII)?
52	Does the data or information contain Personal Health Information (PHI)?
53	Which EU Member State(s) does the information originate?
54	Data classification category
55	Confidential Data Label (from Policy on Data Classification and Security)
56	International Transfer Destination
57	Data Protection Impct Assessment Performed?
58	If yes, was it approved for processing?
59	If GDPR system, select the lawful basis for processing
60	How is the Data Subject's Consent obtained and tracked?
61	Assessment of the necessity and proportionality of the processing
62	An assessment of the risks to the rights and freedoms of the data subject
63	The measures envisioned to mitigate the risks
64	Describe the safeguards and security measures to employed that demonstrate compliance
65	Indication of Privacy By Design and Default measures
66	Collection Method
67	Type of Format
68	Technical and organisational security measures applied
69	What is the number of months the information is retained in production? If years please answer in number of months (years multipled by 12)
70	If a third party provider is used, describe the retention period applied to the information (number of years, size quota, etc.)
71	Record Series Association

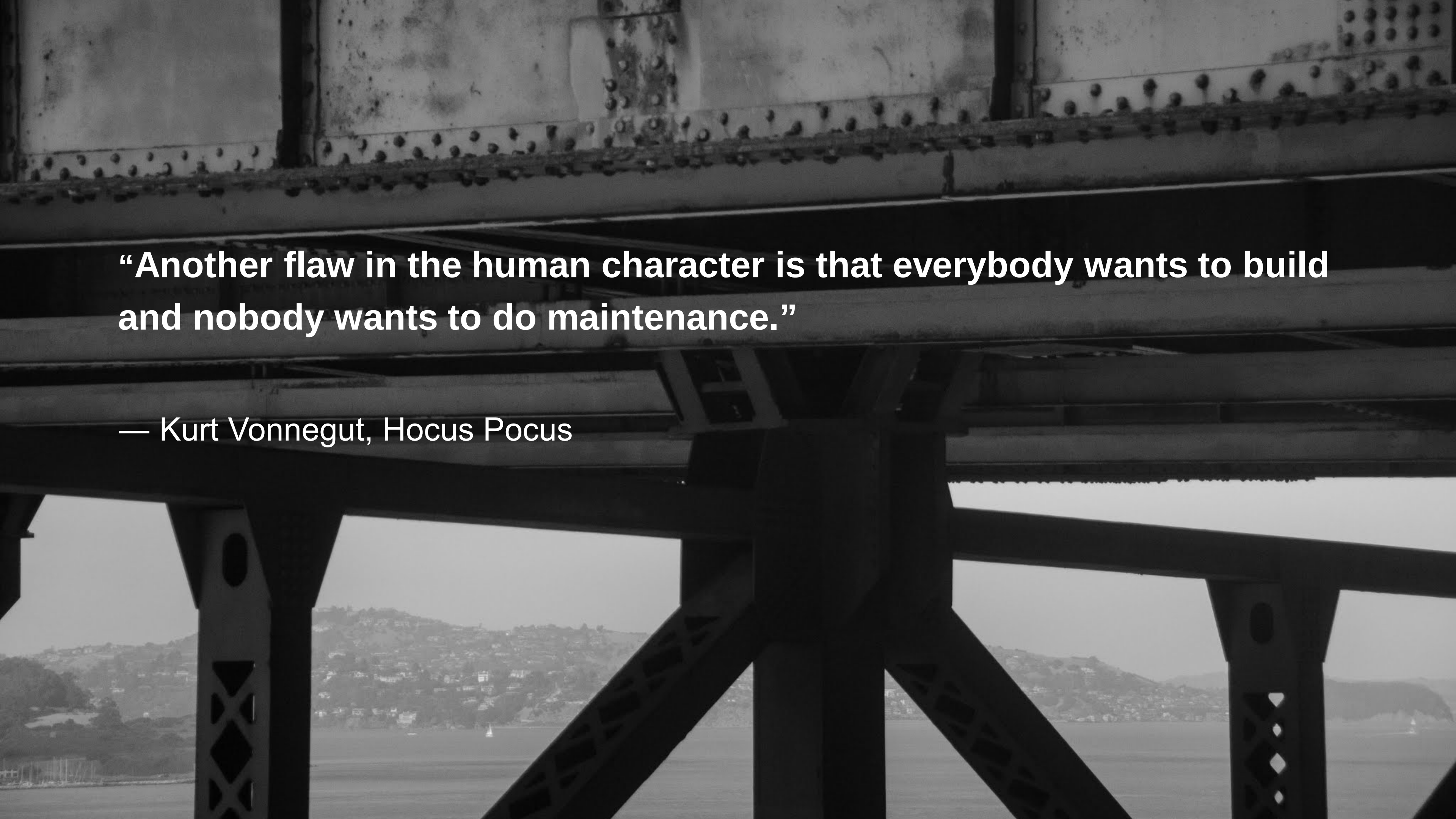
PITFALLS!!

Version Control

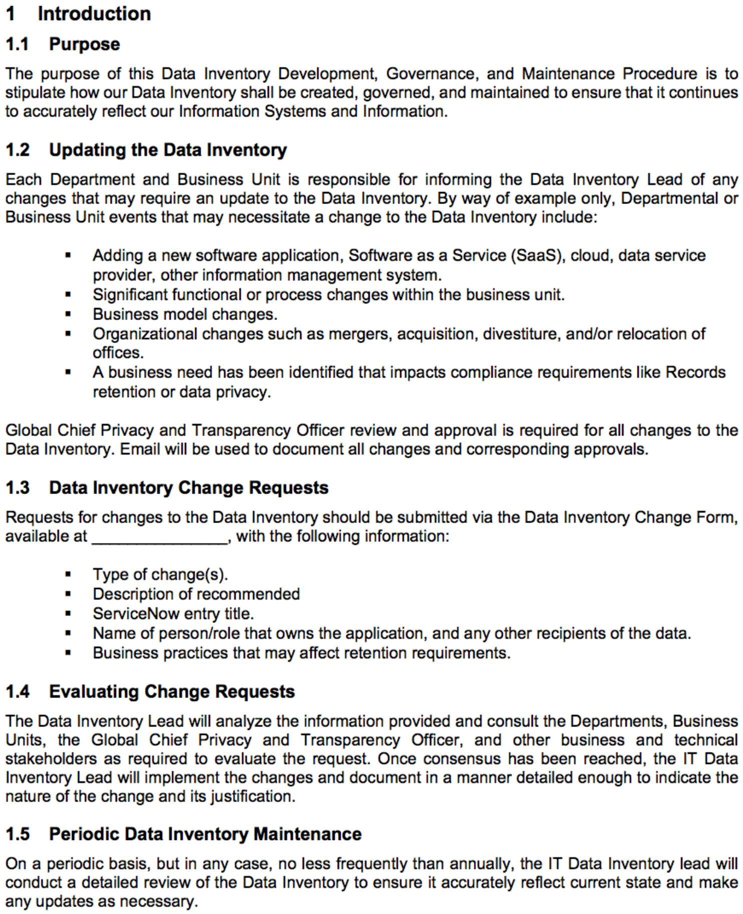
Too much detail

Too little detail

No end in sight



> **“Another flaw in the human character is that everybody wants to build and nobody wants to do maintenance.”**
>
> — Kurt Vonnegut, Hocus Pocus



1 Introduction

1.1 Purpose

The purpose of this Data Inventory Development, Governance, and Maintenance Procedure is to stipulate how our Data Inventory shall be created, governed, and maintained to ensure that it continues to accurately reflect our Information Systems and Information.

1.2 Updating the Data Inventory

Each Department and Business Unit is responsible for informing the Data Inventory Lead of any changes that may require an update to the Data Inventory. By way of example only, Departmental or Business Unit events that may necessitate a change to the Data Inventory include:

- Adding a new software application, Software as a Service (SaaS), cloud, data service provider, other information management system.
- Significant functional or process changes within the business unit.
- Business model changes.
- Organizational changes such as mergers, acquisition, divestiture, and/or relocation of offices.
- A business need has been identified that impacts compliance requirements like Records retention or data privacy.

Global Chief Privacy and Transparency Officer review and approval is required for all changes to the Data Inventory. Email will be used to document all changes and corresponding approvals.

1.3 Data Inventory Change Requests

Requests for changes to the Data Inventory should be submitted via the Data Inventory Change Form, available at ________________, with the following information:

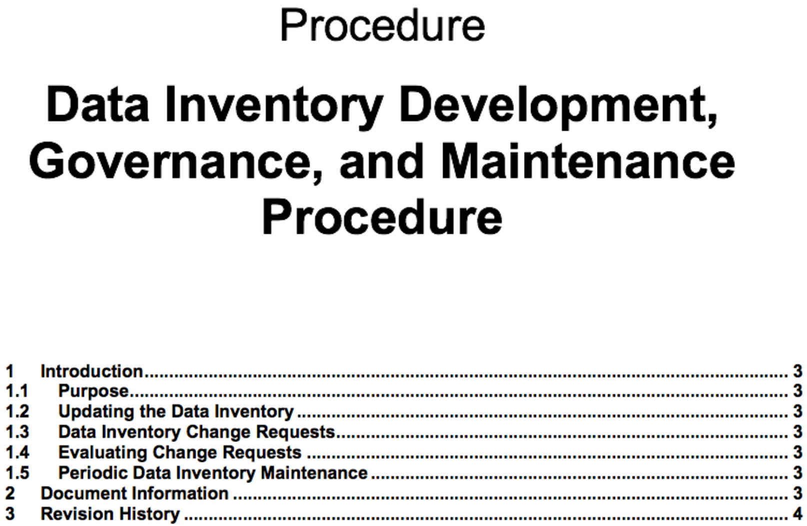
- Type of change(s).
- Description of recommended
- ServiceNow entry title.
- Name of person/role that owns the application, and any other recipients of the data.
- Business practices that may affect retention requirements.

1.4 Evaluating Change Requests

The Data Inventory Lead will analyze the information provided and consult the Departments, Business Units, the Global Chief Privacy and Transparency Officer, and other business and technical stakeholders as required to evaluate the request. Once consensus has been reached, the IT Data Inventory Lead will implement the changes and document in a manner detailed enough to indicate the nature of the change and its justification.

1.5 Periodic Data Inventory Maintenance

On a periodic basis, but in any case, no less frequently than annually, the IT Data Inventory lead will conduct a detailed review of the Data Inventory to ensure it accurately reflect current state and make any updates as necessary.



Procedure

Data Inventory Development, Governance, and Maintenance Procedure

Maintenance & Governance

Corporate Governance: Who is in Charge?

- CISO vs. CPO
  - The role of the CISO and the CPO differ in reporting structure, scope, and authority.
- CPO
  - The CPO is responsible for the vision, strategy, and program regarding use of personal information.
  - CPO often reports to either a general counsel, chief compliance officer and may have a dotted line to a board of directors.
- CISO
  - The CISO is responsible for the vision, strategy, and program to ensure protection of information assets, and technologies.
  - CISO may report to either the chief technology officer, chief information officer (CIO), and may also have a dotted line to the board.

Separate and Overlapping Governance Domains

CPO

- External privacy policy
- Internal privacy policies
- Data classification procedures
- DPIA/Privacy Register
- Data subject access request procedures
- Privacy notices
- Etc.

BOTH

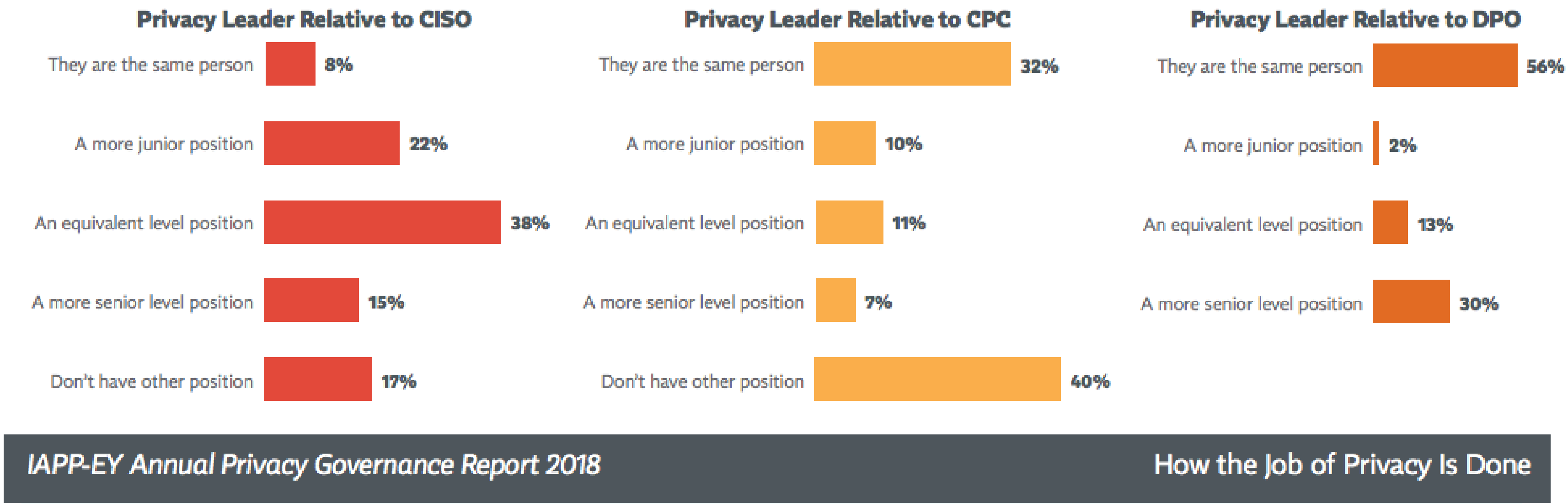
- Vendor evaluation and management
- Data breach and incident response
- Data sensitivity classification and management
- Employee training and compliance
- Etc.

CISO

- Information protection policy
- Security standards and requirements;
- Data Loss Prevention;
- Device/system inventories and risk classification
- Perimeter security
- Access control
- Etc.

Current State

- 43 percent of privacy leaders are located in legal and 61 percent handled other domains aside from privacy



IAPP-EY Annual Privacy Governance Report 2018

How the Job of Privacy Is Done

Jay Brudz

Partner | Washington, D.C.

jay.brudz@dbr.com
Phone: (202) 230-5195

About

Jay Brudz builds and manages world class e-discovery operations, internal compliance and FCPA investigations and develops enterprise-level information governance best practices. He is co-chair of the Information Governance and eDiscovery Group. In that capacity he acts as e-discovery counsel on major complex litigation matters. Using his technical experience in digital forensics and network security, Jay assists clients with information security counselling, including breach response, policy development and cyber risk evaluations. He also serves as executive managing director of the firm's e-discovery subsidiary, Tritura Information Governance LLC, which provides state of the art e-discovery technology and services to the firm's clients.

Jay previously served in several roles focusing on the intersection of applied technology and law, including as senior counsel for legal technology at General Electric where he created and led their corporate e-discovery center supporting more than 1,200 attorneys. In this role he was also responsible for all corporate technology initiatives within GE's legal operation, including the successful implementation of legal hold, e-billing, insider trading compliance, intranet, and patent docketing systems.

Jay also previously served as president and senior forensic consultant of Verabit, where he conducted computer forensic investigations and provided expert consultation and testimony in cases ranging from employee misappropriation of trade secrets to FCPA investigations. He also taught computer crime and network security at the University of New Haven. Prior to that, he was a system architect and lead developer for a database backed Web-based development company specializing in creating customized systems for corporate legal operations. Jay is an accomplished Java, PHP, VisualBasic and PL-SQL programmer and has experience with many other technologies. He is a U.S. Army veteran.

Areas of Focus

Services

- eDiscovery
- Information Governance
- Information Privacy, Security and Governance
- Litigation
- Information Privacy
- Information Security

Industries

- Energy

Credentials

Bar Admissions

- Connecticut
- District of Columbia

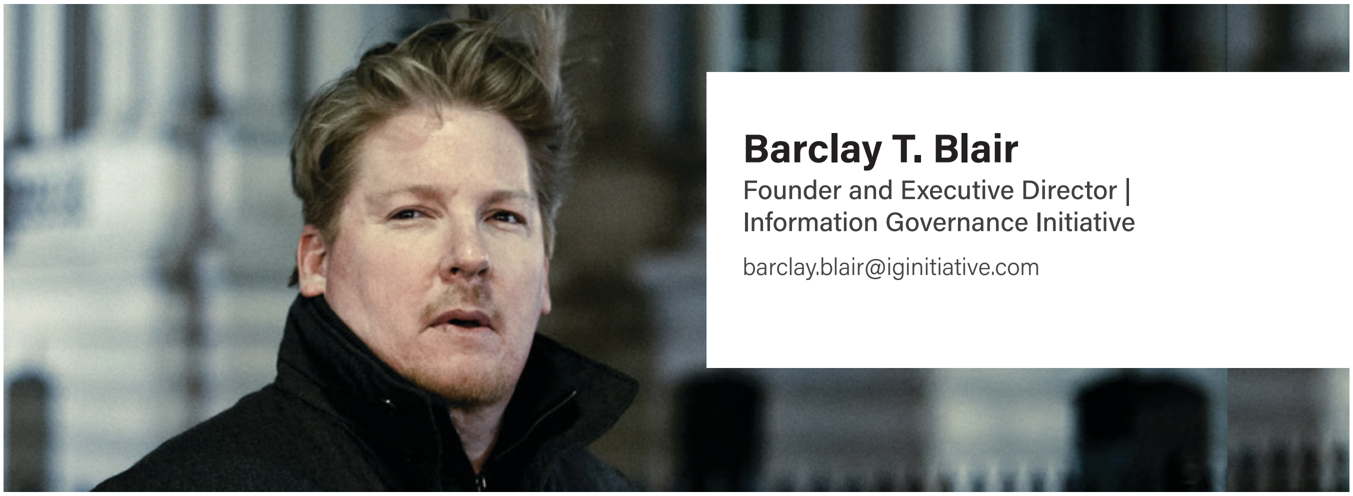
Education

- University of Connecticut School of Law, J.D.
- University of Connecticut, B.A., *cum laude*

Organizations

- Connecticut Bar Association
- District of Columbia Bar Association

DrinkerBiddle®



Barclay T. Blair

Founder and Executive Director |
Information Governance Initiative

barclay.blair@iginitiative.com

About

Barclay T. Blair is an advisor to Fortune 500 companies, technology providers, and government institutions across the globe, and is an speaker, author, and internationally recognized authority on Information Governance. Barclay has led several high-profile consulting engagements at the world's leading institutions to help them globally transform the way they manage information. He is the president and founder of ViaLumina and the Executive Director and Founder of the Information Governance Initiative.

Barclay is the award-winning author of the books Information Nation: Seven Keys to Information Management Compliance; Information Nation Warrior; and Privacy Nation. Barclay has written and edited dozens of publications, speaks internationally on information management compliance issues, and has instructed at George Washington University. Barclay has also edited and contributed to several books, including: Email Rules; Secure Electronic Commerce; and Professional XML. Barclay is currently writing Information Governance for Dummies.

Barclay has presented to industry groups such as the Innovation Enterprise Big Data Summit, Financial Services Roundtable, American Bar Association, American Counsel of Life Insurers, Legal Tech, BNA Litigation Forum, the World Wide Web Consortium (W3C), ARMA International, and the Society of Quality Assurance. In addition, Barclay speaks at dozens of conferences and events each year. Barclay is frequently interviewed by media outlets about information governance.

Areas of Focus

Services

- Information Governan