Mitigating Data Privacy & Security Risks at the Contractual and Insurance Level

July 10, 2024

Presented by: Ben Milam & Brett Lawrence

Agenda

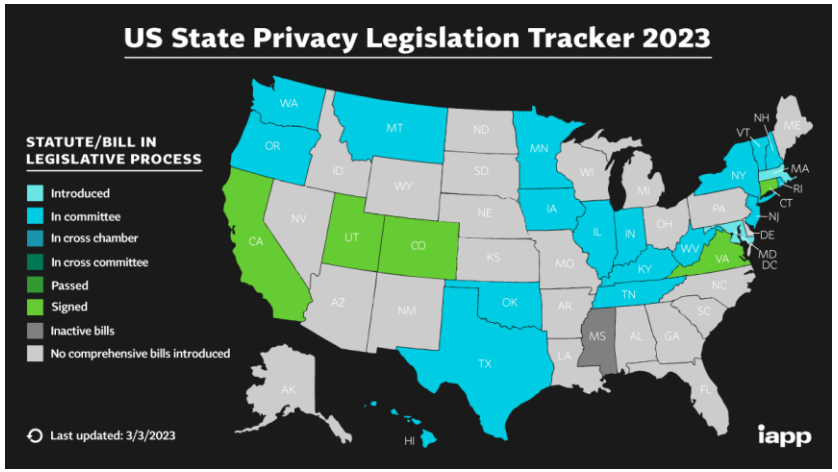
1. The growing privacy landscape
2. Litigation & enforcement considerations
3. Contractual requirements & best practices
4. Insurance for data privacy investigations and penalties
5. Securing insurance requirements in commercial contracts

Bradley

THE GROWING PRIVACY LAW LANDSCAPE

Bradley

The Privacy Law Race Has Not Stopped

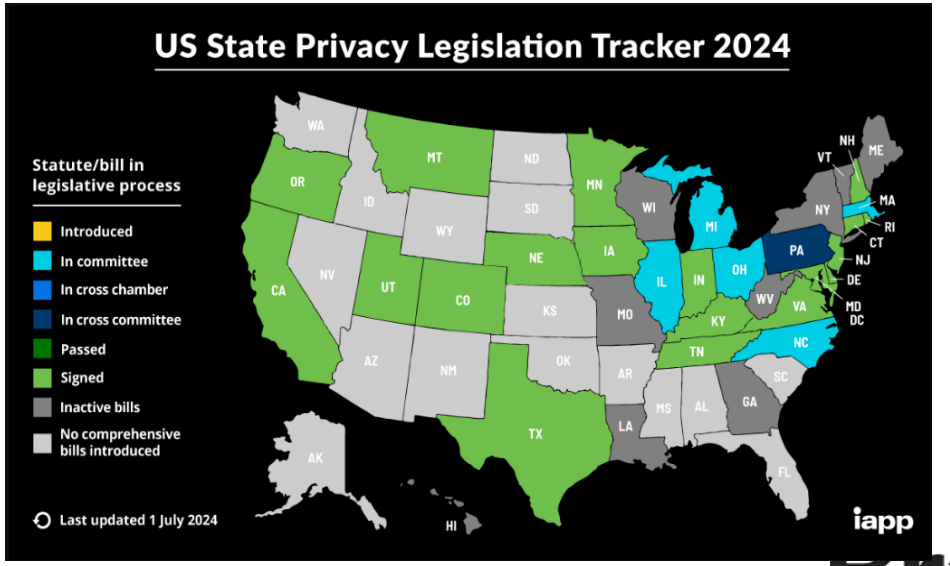


March 2023

5 States

July 2024

19 States



Bradley

The Privacy Law Race Has Not Stopped (Cont'd)

Illinois	SB 3517	Privacy Rights Act
	HB 5581	Illinois Privacy Rights Act
Massachusetts	S 2770	Massachusetts Data Privacy Act
	H 83	Massachusetts Data Privacy Protection Act (C)
	S 25	
	H 60	Massachusetts Information Privacy and Security Act (C)
	S 227	
	HD 3245	Internet Bill of Rights
Michigan	SB 659	Personal Data Privacy Act
North Carolina	SB 525	North Carolina Consumer Privacy Act
Ohio	HB 345	Ohio Personal Privacy Act
Pennsylvania	HB 1947	Consumer Data Privacy Act
	HB 1201	Consumer Data Privacy Act

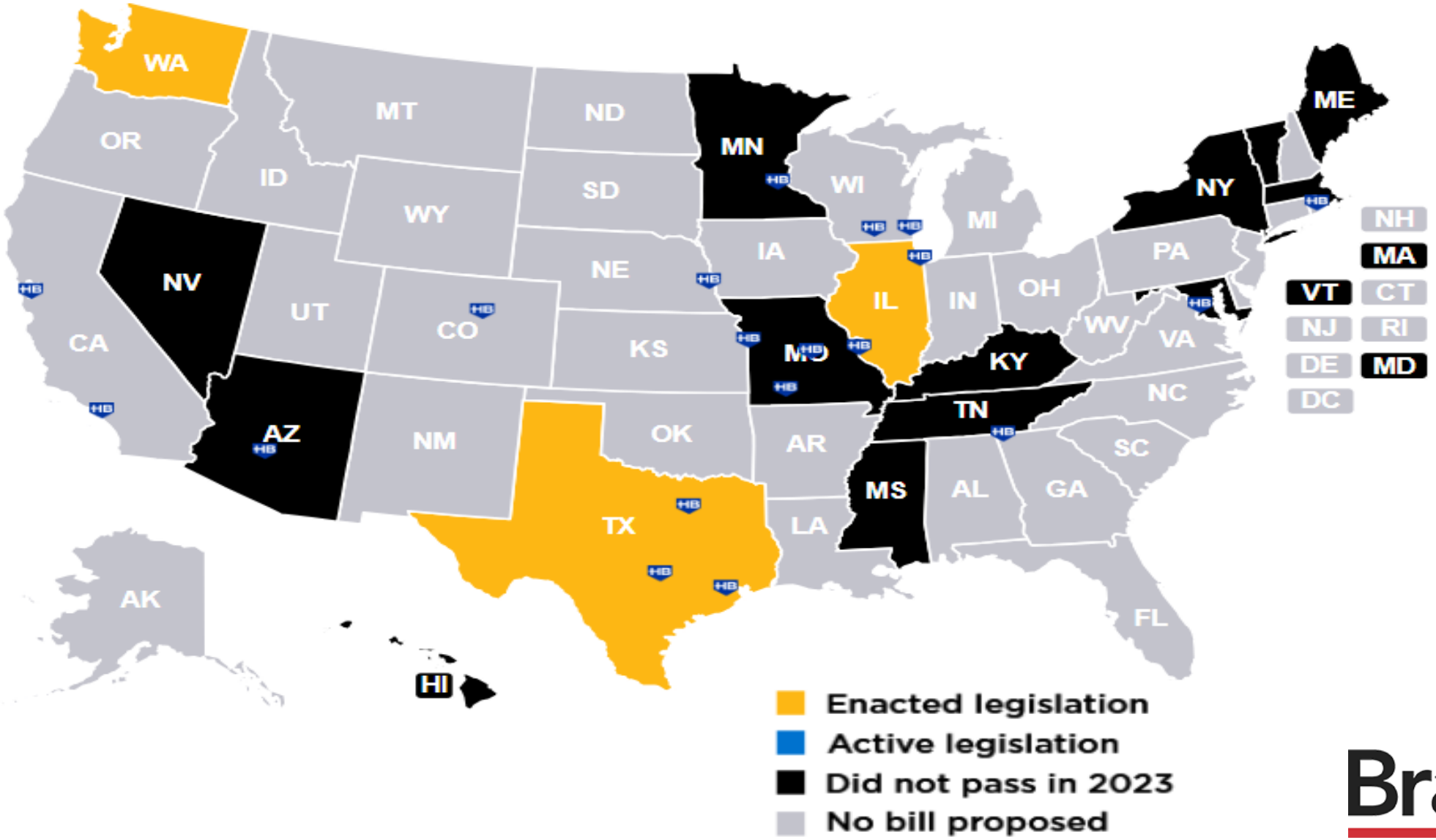
6 states with pending legislation

Georgia	SB 473	Georgia Consumer Privacy Protection Act
Hawaii	SB 3018	Consumer Data Protection Act
Kentucky	SB 15	Kentucky Consumer Data Protection Act
	HB 24	
Louisiana	HB 947	Louisiana Consumer Privacy Act
Maine	LD 1973	Maine Consumer Privacy Act
	LD 1977	Data Privacy and Protection Act
Minnesota	HB 1367	
	SB 950	(C)
	HB 1892	
Missouri	SB 1501	
	SB 731	
New York	SB 3162	(C)
	A 4374	
	SB 365	New York Privacy Act (C)
	A 3593	
	SB 5555	It's Your Data Act
	A 2587	New York Data Protection Act
	A 6319	American Data Privacy and Protection Act
	A 3308	Digital Fairness Act
	SB 2277	
Vermont	H 121	Vermont Data Privacy Act (C)
	S 269	
West Virginia	HB 5698	
	HB 5112	Consumer Data Protection Act
Wisconsin	AB 466	(C)
	SB 642	

11 states this year have attempted privacy legislation

Bradley

Burgeoning State Biometric Privacy Legislation



Bradley

Rollout Schedule

Effective Date	States
January 1, 2020	California
January 1, 2023	Virginia
July 1, 2023	Colorado, Connecticut
December 31, 2023	Utah
July 1, 2024	Oregon, Texas
October 1, 2024	Montana
January 1, 2025	Delaware, Iowa, Nebraska, New Hampshire
January 15, 2025	New Jersey
July 1, 2025	Tennessee
July 31, 2025	Minnesota
October 1, 2025	Maryland
January 1, 2026	Indiana, Kentucky, Rhode Island

Bradley

Notable State Laws

California – CCPA/CPRA

$100-750 per consumer

Illinois – Biometric Information Privacy Act (BIPA)

Negligent violation: $1,000 per violation

Intentional or reckless violation: $5,000 per violation

Florida – "Mini" TCPA

$500 or actual damages, whichever is greater. Treble damages available

Washington – My Health My Data Act (MHMDA)

Individuals may file under WA Consumer Protection Act

State Wiretapping laws

Bradley

Federal Laws

- **Health Insurance Portability & Accountability Act** (HIPAA)
- **Gramm–Leach–Bliley Act** (GLBA)
- **Telephone Consumer Protection Act** (TCPA)
- **Video Privacy Protection Act of 1988** (VPPA)
- **The Privacy Act of 1974**
- **Children's Online Privacy Protection Act** (COPPA)
- **Fair and Accurate Credit Transactions Act of 2003** (FACTA)
- **Family Educational Rights and Privacy Act** (FERPA)

Bradley

Litigation & Enforcement Considerations

- **Class Actions on the Rise**
  - Data breaches
  - Tracking technology/Pixel Litigation
  - Inadvertent use cases (biometric laws)
  - Common law torts (invasion of privacy, intrusion upon seclusion)
- **Square-Peg-Round-Hole Claims**
  - Wiretapping Claims
  - VPPA Claims
  - Song-Beverly Credit Card Act Claims
- **State and Federal Enforcement Actions**
  - FTC
  - State Attorneys General

Bradley

Illinois's BIPA Trends

- ***Cothron v. White Castle System, Inc*. (2023)**
  - In a 4-3 decision, the Illinois Supreme Court held that "[a] party violates … [BIPA] when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection."
    - **In other words: a BIPA violation occurs each time an entity collects or disclose biometric data without consent, not just the first time (defendant theoretically would've had to pay billions in damages)**
  - **BUT** the Court said that it "appears that the General Assembly chose to make [statutory] damages discretionary rather than mandatory under the Act."
  - **Filing of cases jumped 65% two months after this ruling.**
  - Implicates employee data (fingerprint scans, retina scans, etc.)

Bradley

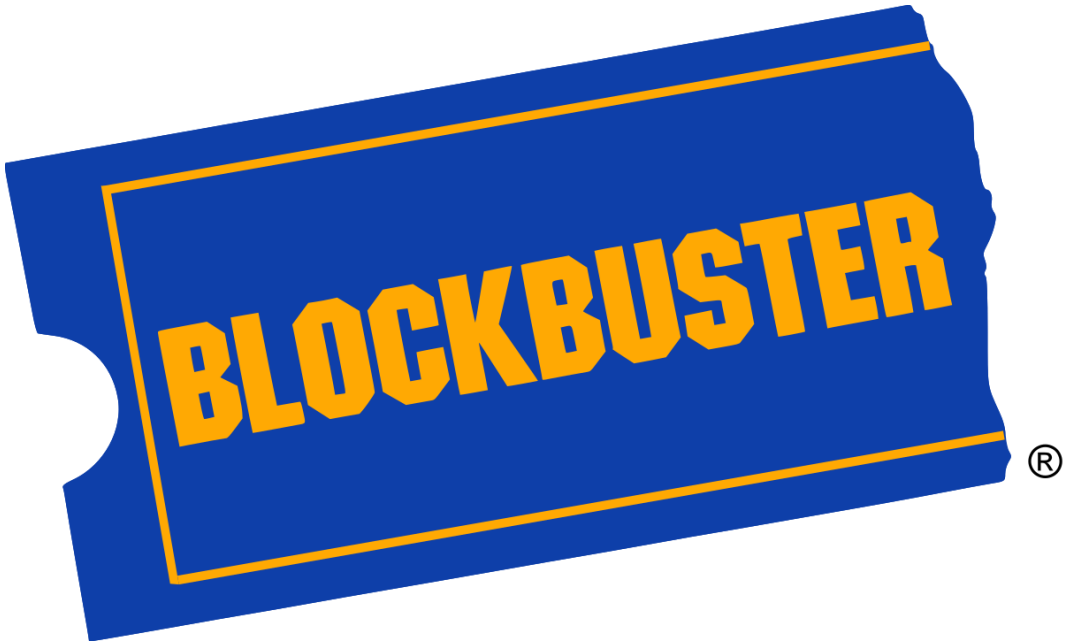
Wiretapping Cases

- **Claims are related to third-party tech on websites**
  - Session replay
  - Chatbot
  - AdTech
  - Keystroke
- **Impacting all industries**
  - Financial services, clothing/retail, health care, automotive, etc.

Bradley

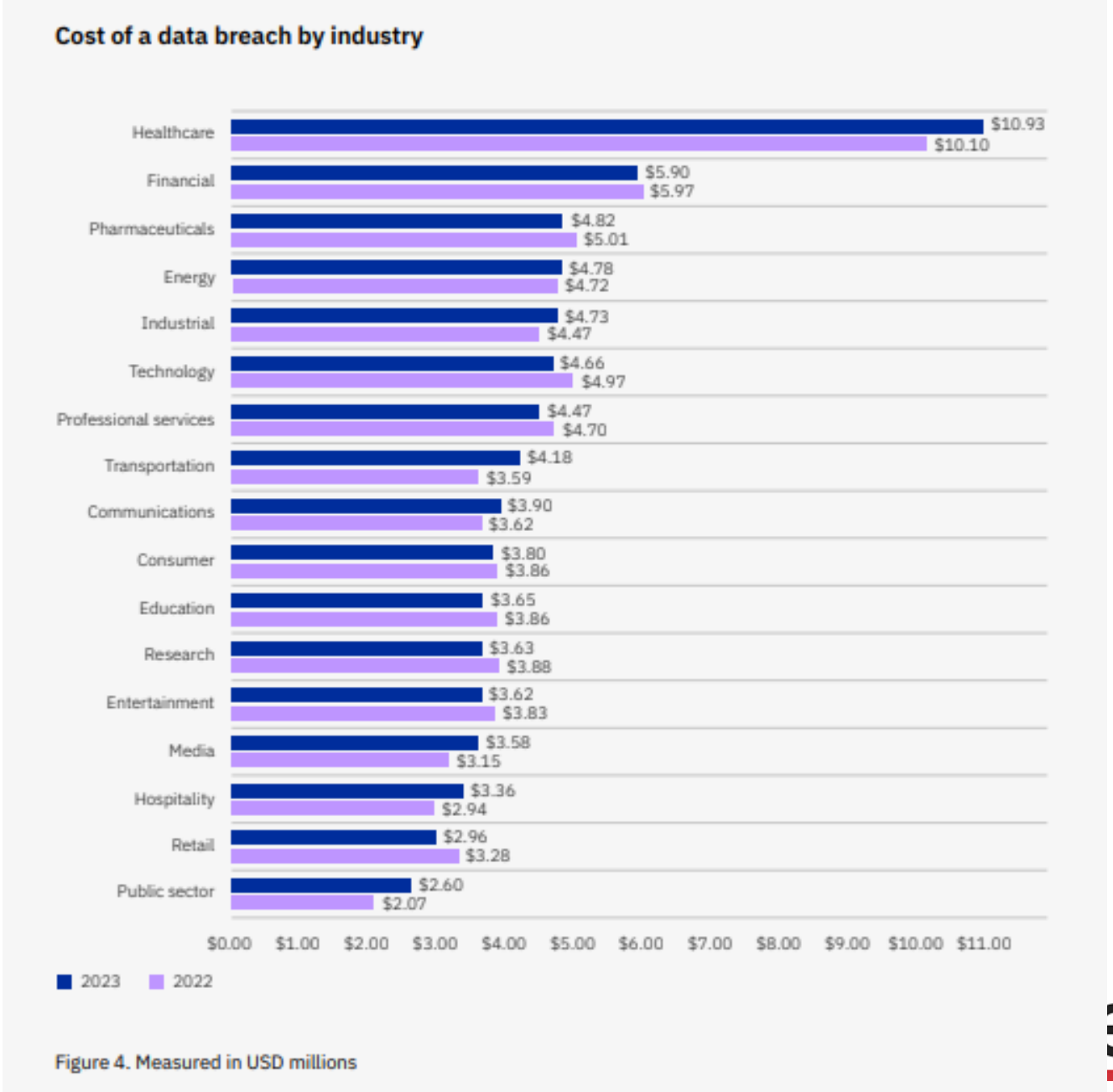
Video Privacy Protection Act ("VPPA")

- **Originally enacted to preserve privacy rights of video rentals**
- **However "video tape service provider" has broad definition to include those engaged in the business of "audio/visual materials".**
- **Claims, including class actions, have recently been filed against website owners who have imbedded videos (such as You Tube) or video content.**
- **Because these videos often overlap with website tracking technologies, the claim is centered on the collection/disclosure of PII associated with watching the video.**
- **Claims are popular because the VPPA contains a minimum damage provision of $2,500 / person / violation. With potential for large class of individuals.**
- **Widespread use of online marketing trackers (i.e. Facebook pixel) makes it easier for claims to survive early dismissal.**



Bradley

Average Cost of a Data Breach By Industry



Source: IBM Cost of a Data Breach Report 2023

CONTRACTUAL REQUIREMENTS & BEST PRACTICES

Bradley

Where Do I Start?

- **Determine relationship between you and the contracting party.**
  - Controller-Processor
  - Controller-Controller
  - Processor-Processor
- **What and how much consumer data is involved (if at all)?**
  - Commercial/employment data v. personal/household data
- **Understanding legal compliance issues versus business risk issues**

Bradley

CCPA Contract Requirements

Service Providers/Contractors

- Specific description of the business purposes.
- Service provider/contractor must comply with applicable CCPA parts.
- Business can take steps to check if service provider is properly using personal information.
- Business can stop and remediate service provider's/contractor's unauthorized use of personal information.
- Service provider/contractor must notify business after it determines that it cannot follow CCPA.
- Cannot "sell" or "share" personal information.
- Cannot retain or use personal information for any purpose but the business purpose.
- Cannot retain or use personal information outside the direct business relationship with business.
- Cannot combine personal information received from business with information received from other sources.
- Must comply/cooperate with a business's notification to comply with a verified consumer request.

"Third Parties"

- Description of the limited and specified purpose(s).
- Business is only disclosing personal information for limited and specified purposes.
- Third party must comply with all applicable CCPA parts.
- Business can take steps to check if third party is properly using personal information.
- Business can stop and remediate third party's unauthorized use of personal information.
- Third party must notify business after it determines that it cannot follow CCPA.
- Cannot use personal information other than for the purposes described in the contract.

Cal. Code Regs. Tit. 11, §§ 7051, 7053

Contractual Requirements for the Other States

1. Instructions for processing personal data
2. Appropriate technical and organization security measures
3. Description of the nature and purpose of the processing,
4. The type of personal data subject to processing,
5. The duration of the processing,
6. Description of the parties' rights and obligations
7. Confidentiality provisions (personnel and subcontractors)
8. Contractual requirements for subcontractors assisting the processor
9. Opportunity for the business to object to the use of a subcontractor by a vendor
10. Delete or return the personal data after the agreement is terminated or the services are no longer being rendered, whichever occurs earlier (subject to exceptions)
11. General audit provisions to ensure legal compliance

Bradley

Contractual Requirements (Cont'd)

Audit Rights

a. Vendor agrees that Client may take reasonable and appropriate steps to ensure that Vendor uses Personal Data in a manner consistent with Client's obligations under applicable Data Protection Laws.

b. Vendor agrees that Client may take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by Vendor.

- Most negotiated
- Flexible
- Designed so parties can tailor specific audit rights afforded to controllers

Bradley

Contractual Requirements (Cont'd)

- Failure to include minimum contractual requirements is not a proper vendor contract for the exchange of personal data
- Risk that the personal data exchanged = violation of law and could lead to subsequent violations

> (e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a), may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.

Cal. Code Regs. Tit. 11, § 7050

Bradley

"Nice to Haves"

Data ownership clarification (de-identified data, aggregated data)

(f) Aggregated Statistics. Notwithstanding anything to the contrary in this Agreement, Provider may monitor Customer's use of the Services and collect and compile Aggregated Statistics. As between Provider and Customer, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are retained solely by Provider. Customer acknowledges that Provider may compile Aggregated Statistics based on Customer Data input into the Services. Customer agrees that Provider may (i) make Aggregated Statistics publicly available in compliance with applicable law, and (ii) use Aggregated Statistics to the extent and in the manner permitted under applicable law[; provided that such Aggregated Statistics do not identify Customer or Customer's Confidential Information.

E. Notwithstanding anything herein to the contrary, Business Associate may not de-identify Protected Health Information unless expressly required to provide services to Company pursuant to the Underlying Agreements.

F. Business Associate may use Protected Health Information to provide Data Aggregation services to Company as permitted by 45 CFR § 164.504(e)(2)(i)(B) to the extent expressly required to provide services to Company pursuant to the Underlying Agreements.

Bradley

“Nice to Haves” (Cont’d)

Cooperation requirements

3. RIGHTS OF DATA SUBJECTS

3.1. Data Subject Request. SFDC shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject’s right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a “Data Subject Request”. SFDC shall not respond to a Data Subject Request itself, except that Customer authorizes SFDC to redirect the Data Subject Request as necessary to allow Customer to respond directly.

3.2. Required Assistance. Taking into account the nature of the Processing, SFDC shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3. Additional Assistance. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SFDC shall upon Customer’s request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SFDC is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from SFDC’s provision of such assistance.

Bradley

"Nice to Haves" (Cont'd)

Data breaches & clarifying damages/cost shifting

"Security Breach" means (i) any act or omission that materially compromises the security, confidentiality, or integrity of Personal Data, and especially includes any security incident that does require (or could reasonably be considered to require) Client to notify impacted individuals, law enforcement, and/or regulatory authorities; (ii) a breach or alleged breach of the Agreement or this Addendum relating to such privacy and data security practices; or (iii) a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

- **Notification timeline requirements**
- **Duties to investigate, remediate, and mitigate**
- **Duties to assist the controller in complying with controller's own obligations under applicable laws**

Vendor shall cooperate with Business in the provision of any notification, including but not limited to, affected individuals and governmental authorities. Vendor shall promptly reimburse Business for all reasonable costs and expenses incurred by Business with respect to providing notification of a Security Breach involving Vendor, including without limitation costs and expenses related to attorneys' and consultants' fees, printing, postage, providing identity theft protection, and the establishment of hotlines.

Bradley

“Nice to Haves” (Cont’d)

Indemnification and [No] Limitations of Liability

- Often limited to infringement claims
- Extend to breaches of the DPA and/or improper use of personal data
- Often limited to direct damages in the form of fees paid by the controller
- Negotiate for super-caps in the liability section
- Clarify what constitutes a “direct damage”
- Can factor insurance limits into the scope of damages afforded

10. LIMITATION OF LIABILITY

A. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL SUMMIT HOSTING OR ITS AFFILIATES, OR ANY OF SUMMIT HOSTING’S RESPECTIVE LICENSORS OR SERVICE PROVIDERS, HAVE ANY LIABILITY ARISING FROM OR RELATED TO CUSTOMER’S USE OF OR INABILITY TO USE THE SERVICES FOR:

(i) PERSONAL INJURY, PROPERTY DAMAGE, LOST PROFITS, COST OF SUBSTITUTE GOODS OR SERVICES, LOSS OR CORRUPTION DATA, LOSS OF GOODWILL, BUSINESS INTERRUPTION, COMPUTER FAILURE OR MALFUNCTION OR ANY OTHER CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL OR PUNITIVE DAMAGES;

Bradley

Limitation of Liability

12.3 Each party's total liability arising under or in connection with this Agreement or any breach or non-performance of it no matter how fundamental (including by reason of that party's negligence) in contract, tort or otherwise shall be limited to 1 year contract value.

FOR DAMAGES ARISING OUT OF A DATA PROTECTION CLAIM, EACH PARTY'S TOTAL LIABILITY FOR ANY REASON AND UPON ANY CAUSE OF ACTION EXCEPT FOR CLAIMS FOR PAYMENT OF FEES REQUIRED BY THE AGREEMENT, IS LIMITED TO THREE TIMES (3X) ALL FEES PAID TO VENDOR BY CLIENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO THE LIABILITY. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT. A DATA PROTECTION CLAIM IS DEFINED AS: (a) ANY CLAIM ARISING

Bradley

INSURANCE FOR REGULATORY INVESTIGATIONS AND PENALTIES

Bradley

“A La Carte” Approach to Cyber

First Party Coverage

- Post Breach Response
  - Crisis management
  - Privacy notification
- Time Element
  - Business interruption
  - Extra expense
- Theft/Fraud
  - Data assets
  - Cyber extortion
  - Computer fraud
  - Funds transfer fraud
  - Social engineering

Third Party Coverage

- Information security and privacy liability
- Regulatory defense and penalties
- Payment card industry fines and assessments
- Website media liability
- Bodily injury and property damage

Bradley

Coverage for Regulatory Risks

- Cyber policy may offer coverage for investigations, fines and penalties by data privacy regulators
- Covers costs to investigate and respond to regulatory inquiries
- Many policies also cover regulatory fines and penalties

Bradley

Triggers for Regulatory Coverage

- Regulatory investigation into unauthorized disclosure of confidential information or violation of a data privacy regulation
- Commencement of administrative enforcement proceeding
- Where coverage not yet triggered but anticipated, “notice of circumstance” to insurer may secure coverage under current policy period

Bradley

INCORPORATING INSURANCE REQUIREMENTS IN COMMERCIAL CONTRACTS

Bradley

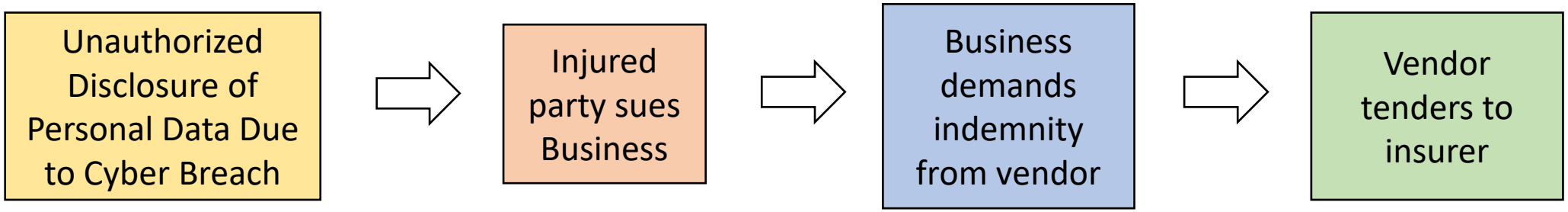
Your Vendor Agreement

- Indemnity provisions will decide who bears risk of loss in event of breach
- Ideally, you want full risk transfer to vendor but may not be commercially realistic
- Vendor may demand liability cap, carve-outs, or negligence standard
- Vendor should have financial backstop for indemnity obligation, such as insurance

Bradley

Insurance Requirements Should Follow Desired Risk Transfer

- IT vendor agrees to indemnity provision in its contract
- Insurance should be purchased that will provide financial backing for contractually assumed indemnification
- Business seeks indemnification from the vendor
- Vendor tenders defense and liabilities to insurer



Bradley

What Insurance to Require From Vendors

- Technology Errors and Omissions
- Cyber and data privacy liability
- First party coverages may also speed vendor's recovery and reduce impact on your business

Bradley

Additional Insured Status

- Protects Additional Insured from Named Insured's negligence
- Covers Additional Insured for liability arising from Named Insured's acts and omissions (but not from Additional Insured's sole negligence)
- Benefits:
  - Coverage without premium
  - No responsibility for deductibles or SIRs
  - No erosion of AI's policies
  - By name or category (blanket)
- Generally not available for E&O

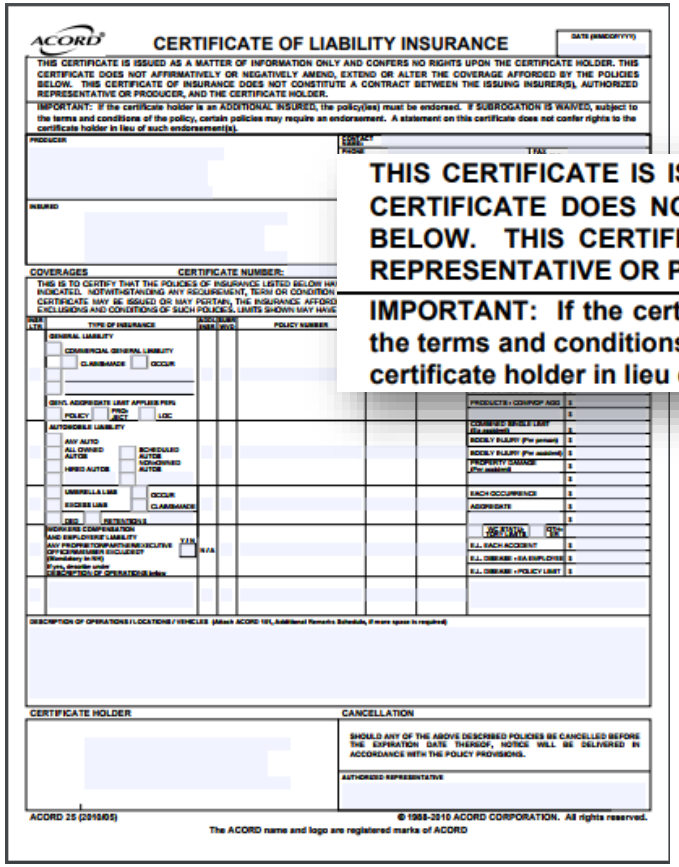
Bradley

Minimum Insurer Rating

- Require insurer with specified minimum quality and size rating by third-party rating agency such as A.M. Best, Moody's, S&P
  - "the insurer shall be rated not less than A-VII by A.M. Best's rating organization"
- Address effect of rating downgrade
  - Allow time to obtain substitute coverage?
  - Additional premium cost?

Bradley

Certificate of Insurance Not Binding



ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

CONTACT NAME:
PHONE (A/C, No, Ext):
FAX (A/C, No):

INSURED

COVERAGES

CERTIFICATE NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HA
INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION
CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORD
EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	GENERAL LIABILITY						EACH OCCURRENCE $
	COMMERCIAL GENERAL LIABILITY						DAMAGE TO RENTED PREMISES (Ea occurrence) $
	CLAIMS-MADE OCCUR						MED EXP (Any one person) $
							PERSONAL & ADV INJURY $
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE $
	POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG $
	AUTOMOBILE LIABILITY						$
	ANY AUTO						COMBINED SINGLE LIMIT (Ea accident) $
	ALL OWNED AUTOS						BODILY INJURY (Per person) $
	SCHEDULED AUTOS						BODILY INJURY (Per accident) $
	HIRED AUTOS						PROPERTY DAMAGE (Per accident) $
	NON-OWNED AUTOS						$
	UMBRELLA LIAB OCCUR						EACH OCCURRENCE $
	EXCESS LIAB CLAIMS-MADE						AGGREGATE $
	DED RETENTION $						$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY						PER STATUTE OTH-ER
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)	Y/N	N/A				E.L. EACH ACCIDENT $
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE $
							E.L. DISEASE - POLICY LIMIT $

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

Bradley

Best Practices for Contract Requirements

- Keep language current
- Ensure appropriate coverages
- Keep provisions consistent
- Include specifics
- Require A.M. Best Rating A:VII or S&P BBB or better
- Include insurer waiver of subrogation
- Request endorsement for 30-day notice of cancellation or require periodic confirmation of coverage

Bradley

QUESTIONS?

Bradley