50 States, 19 Privacy Laws, 1 Headache

Managing Vendor Sourcing and Diligence

Privacy + Security Forum, Spring Academy | May 7, 2025

SafeGuard Privacy™

Speakers

Tony Stein

Principal

Plain Language, Inc.

Rachel Glasser

Chief Privacy Officer

Magnite

Tim Nagle

Associate General Counsel (Privacy), Americas

dentsu

Andy Hepburn

General Counsel

SafeGuard Privacy

Agenda

1. Understanding what's required (the law)
2. Vendor sourcing and diligence in context
3. The vendor's perspective
4. The agency's perspective
5. Actionable Strategies for vendor diligence

Part 1:
Understanding what's required (the law)

Privacy laws that require vendor diligence

Essentially all of them do, but approaches differ.

There's California...

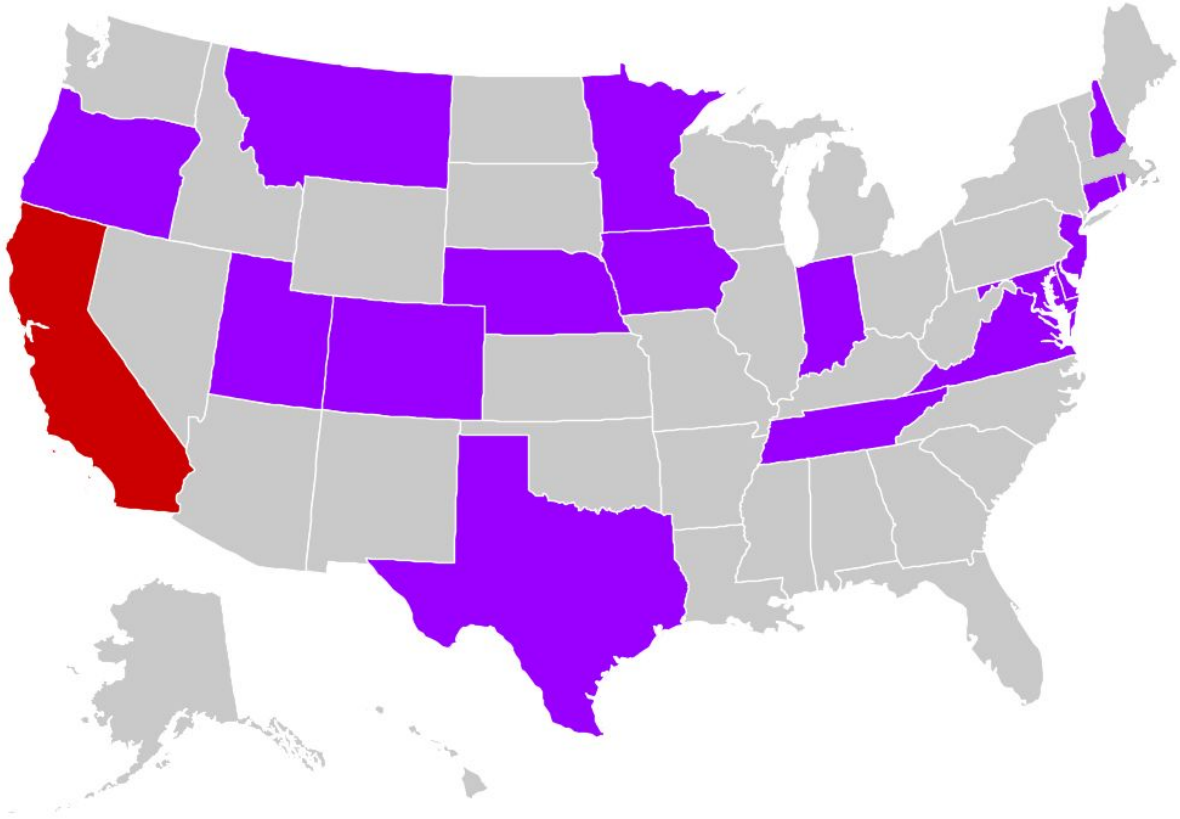
And the 18 other states...

And the FTC Act...

And HIPAA (BAAs)...

And GDPR...

And...



All US states have permissive language, but CA ups the incentive

CCPA Reg §7051 Contract Requirements for Service Providers and Contractors.

(a) The contract shall grant the business **the right** to take reasonable and appropriate steps to ensure that the service provider uses the personal information that it collected in a manner consistent with **the business's obligations** under the CCPA and these regulations.

OK, I have the right, but is it an obligation?

(c) … [A] business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense* that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA ….

*CA Civil Code section 1798.145(i)

Ah do due doo… Are we required or merely encouraged to do diligence?

Surplusage Canon.

If possible, every word and every provision is to be given effect (*verba cum effectu sunt accipienda*). None should be ignored. None should needlessly be given an interpretation that causes it to duplicate another provision or to have no consequence.

> Every word within a statute is there for a purpose and should be given its due significance.
> - US Supreme Court

Source: https://judicature.duke.edu/articles/a-dozen-canons-of-statutory-and-constitutional-text-construction/

Common Sense Question

If I have a statutory diligence right and don't use it, how will a regulator view my compliance efforts?

FTC’s view is clear (or was)

- Recent **Mobilewalla** and **Gravy Analytics** enforcement actions
- Both are data brokers that collect precise geolocation data and sell it for digital advertising purposes
- **Note**: Both had programs to assess data suppliers’ compliance, but
  - **Gravy Analytics** continued using data from suppliers whose questionnaire responses were incomplete or vague
  - **Mobilewalla**’s annual certification process relied on supplier’s self-certification without verification

Takeaway: Assess and Verify

What about (UK) GDPR?

From the UK Information Commissioner's Office FAQ:

What responsibilities does a controller have when using a processor?

- The controller is responsible for assessing that its processor is competent to process personal data in line with the UK GDPR's requirements.
- A controller is primarily responsible for its own compliance and ensuring the compliance of its processors.

Source: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

In case you haven't noticed, the non-CA state privacy laws are mini-GDPRs.

Part 2:
Vendor sourcing and diligence in context

Main Topics

- Risk Management, Generally
- Managing Risks **with** third parties: Risk Management is Relationship Management

A main theme throughout: ***Clarity***

Risk Management, Generally

- Two Definitions
  - Residual Risk = Inherent Risk – Mitigation
  - Risk Appetite is the Residual Risk you can live with

- Therefore, it is essential to understand and document/catalog
  - Your Inherent Risks
  - Your mitigation processes
  - Your management of breaches

Managing Risks with 3rd Parties

- Evaluate Residual Risk for a given 3rd-party relationships based on 3rd-party risk mitigation processes
  - Gap analysis: Compare your risk mitigation with 3rd party's
  - Harmonization of different processes

- Ask: Will the Residual Risks fall within your Risk Appetite?
  - Limit what you have the 3rd party do
  - Reject the 3rd party

You can delegate actions but not responsibilities or risks

3rd-Party Risk Management Requires Relationship Management

3rd third parties must be your risk-management partners.

- Clarify and document expectations:
  If it's not documented, it won't be done
- It is a "Trust-but-verify" situation:
  Communicate and document up front, all that you will be doing to ensure your risks are managed properly by them
- Establish a dispute-resolution process before there are any disputes to resolve

Quick Review

- Know thyself
- Partner with your 3rd parties: harmonize activities
- Communicate oversight
- Clarify, document, communicate early and often

Part 3:
The vendor's perspective

One diligence questionnaire is not like the other

- Vendor pain point: multiple, inconsistent privacy questionnaires that need to be responded. Requires resources.
  - Vendors may also be managing *their* vendors, making the inconsistency even worse
- If you are managing vendors, you could have 7 vendors or 7,000 vendors somewhere in your ecosystem. They could be putting you at risk.
- How do you operationalize? Laws aren't that descriptive or have weak examples, such as "Use Questionnaires." But *what* questionnaires and what is in them?

Streamline and standardize

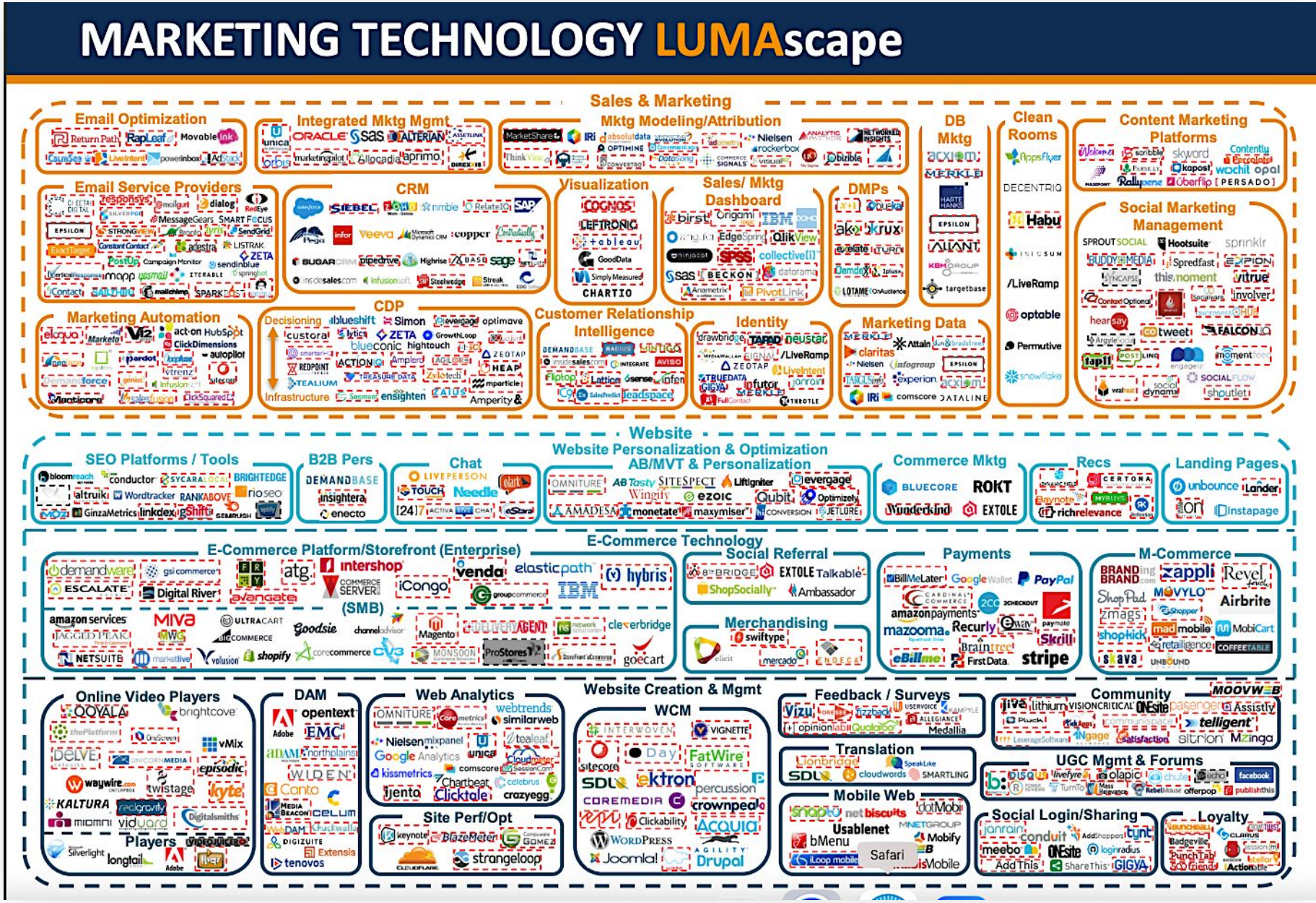
- Manage and set expectations between you and your vendors, and vice versa. Try not to use disparate approaches.
- How to stay consistent in your answers to questionnaires – standardize where you can and create a universal truth of responses.
- There's a requirement to do the work and understand who you are working with. Updating your privacy policy is not enough for both sides of the partnership.

Part 4:
The agency's perspective

From the Financial Perspective

- Focus on identity theft
- Very prescriptive rules
- Consumer Financial Protection Bureau note
  - Limited Applicability of Consumer Financial Protection Act's "Time or Space" Exception with Respect to Digital Marketing Providers

Agencies deal with the entire advertising ecosystem, and it is COMPLEX!



Source: https://www.federalreserve.gov/publications/2024-may-third-party-risk-management.htm#xfigure1-stagesoftherisk-managementl-ec31c8a9r

We deal with all of them!

- Agency-specific challenges include
  - sourcing vendors on behalf of clients
  - intermediary data flows and consumer signal flows
- Regulated industries, like Pharma, have rigorous TPRM obligations – very prescriptive.
  - They are hard, but linear.
  - As compared to digital advertising, where everyone interprets the law to suit their business practices
- Subcontractor challenges and approaches:
  - We want to know who your subs are and be involved in governing them
  - Contract control only
- AI implications?

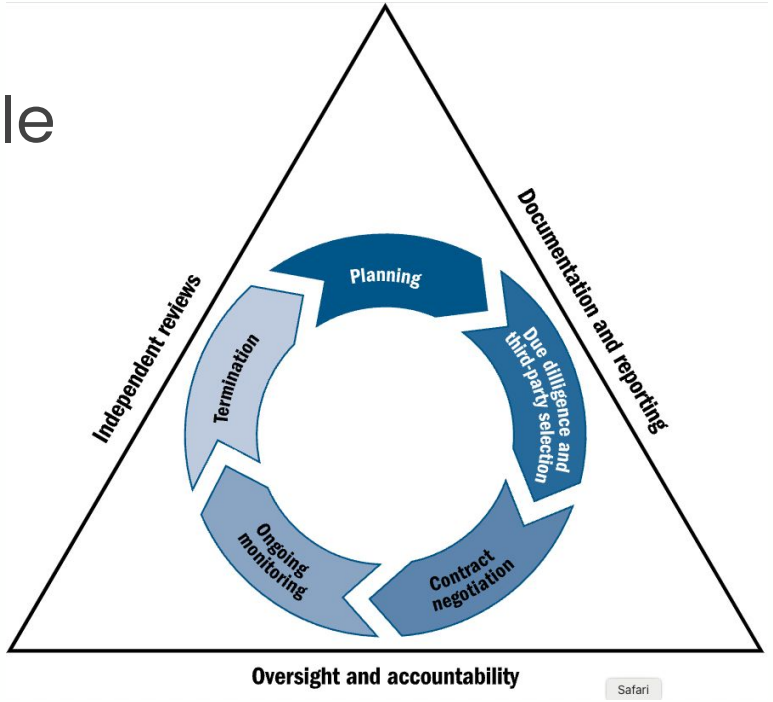
3 points for diligence across the ecosystem:

1. Know the questions you need to ask
2. Know the answers you want to hear
3. Know your plan if you don't get the answers you want

Part 5:
Actionable strategies for vendor diligence

Strategies

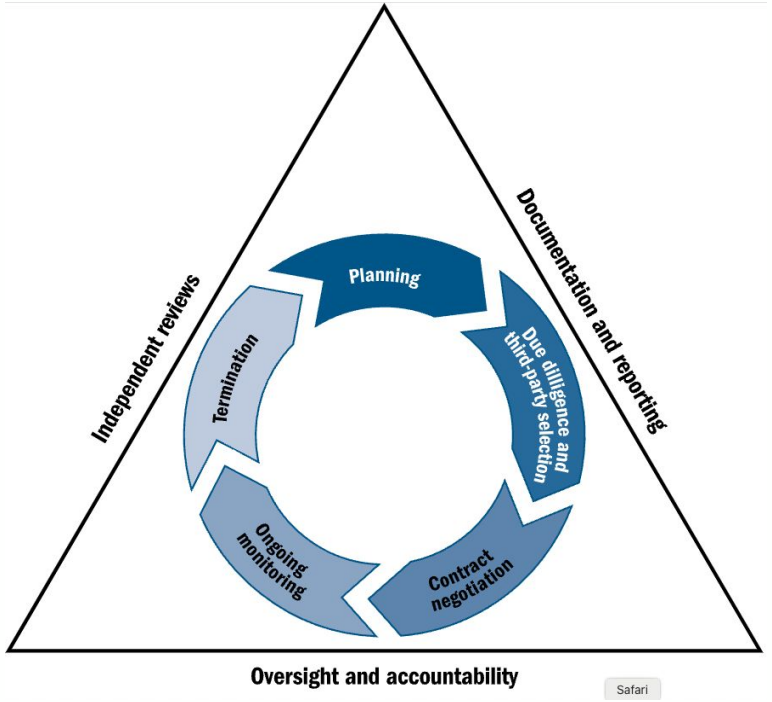
- Just getting started? Good! On the road is better than in the ditch.
- **Know and triage your risk**:
  Privacy, business continuity, etc.
- Leverage your sourcing and governance people and processes. You don't necessarily need to reinvent the wheel.



Source:
https://www.federalreserve.gov/publications/2024-may-third-party-risk-management.htm#xfigure1-stagesoftherisk-managementl-ec31c8a9r

Strategies

- Vendor diligence is a process, not an event. Lather, Rinse, Repeat!
- Make sure you're doing what you say you are: If your contract says you're auditing, you should be auditing.
- **Relationships matter:** Build them, maintain them.



Source: https://www.federalreserve.gov/publications/2024-may-third-party-risk-management.htm#xfigure1-stagesoftherisk-managementl-ec31c8a9r

Questions?

Thank you for attending!

Andy Hepburn: Andy.Hepburn@SafeGuardPrivacy.com

SafeGuard Privacy™

To learn more about SafeGuard Privacy or the IAB Diligence Platform: hello@safeguardprivacy.com

Resources

Resources

- Article: The FTC and the future of third-party due diligence

Sources:

- A Dozen Canons of Statutory and Constitutional Text Construction
- Third-Party Risk Management: A Guide for Community Banks
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR