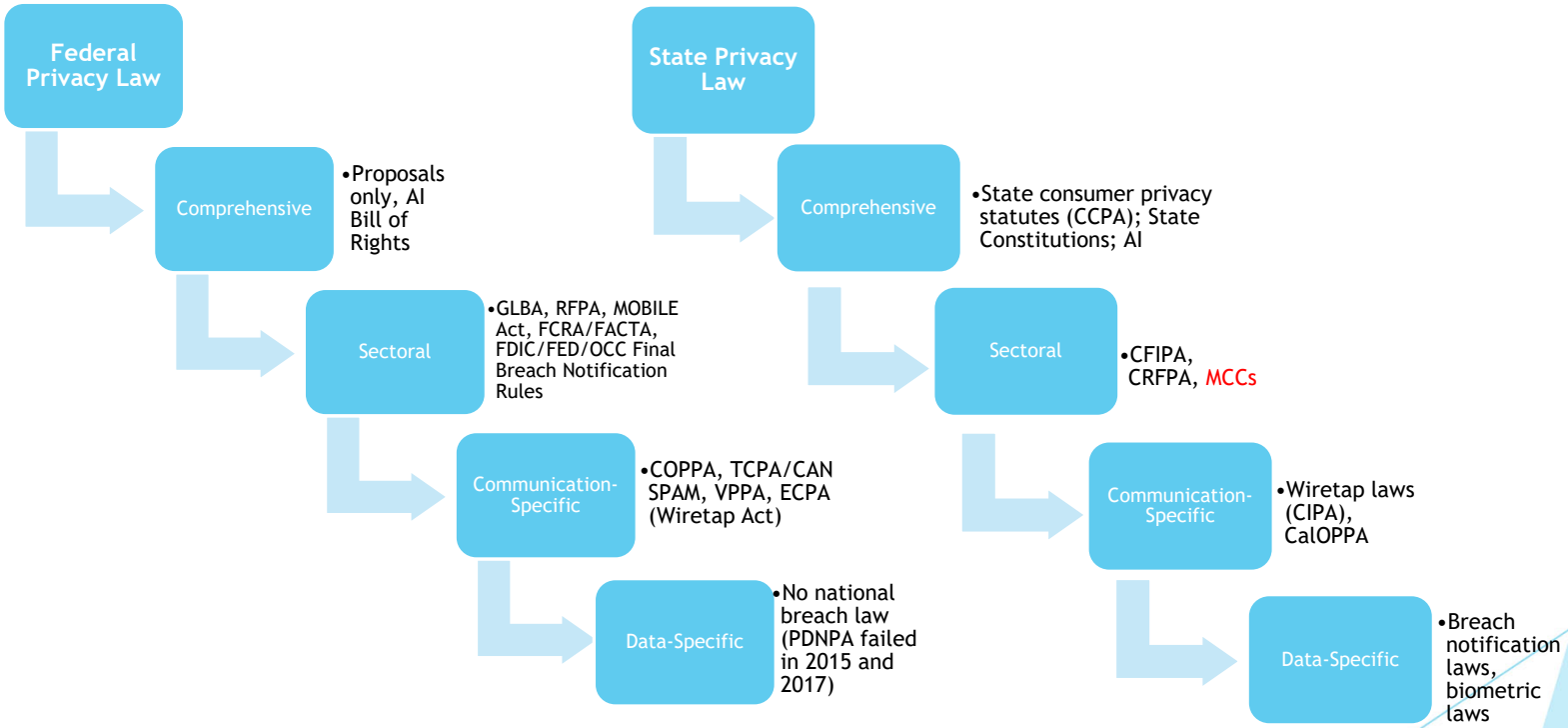
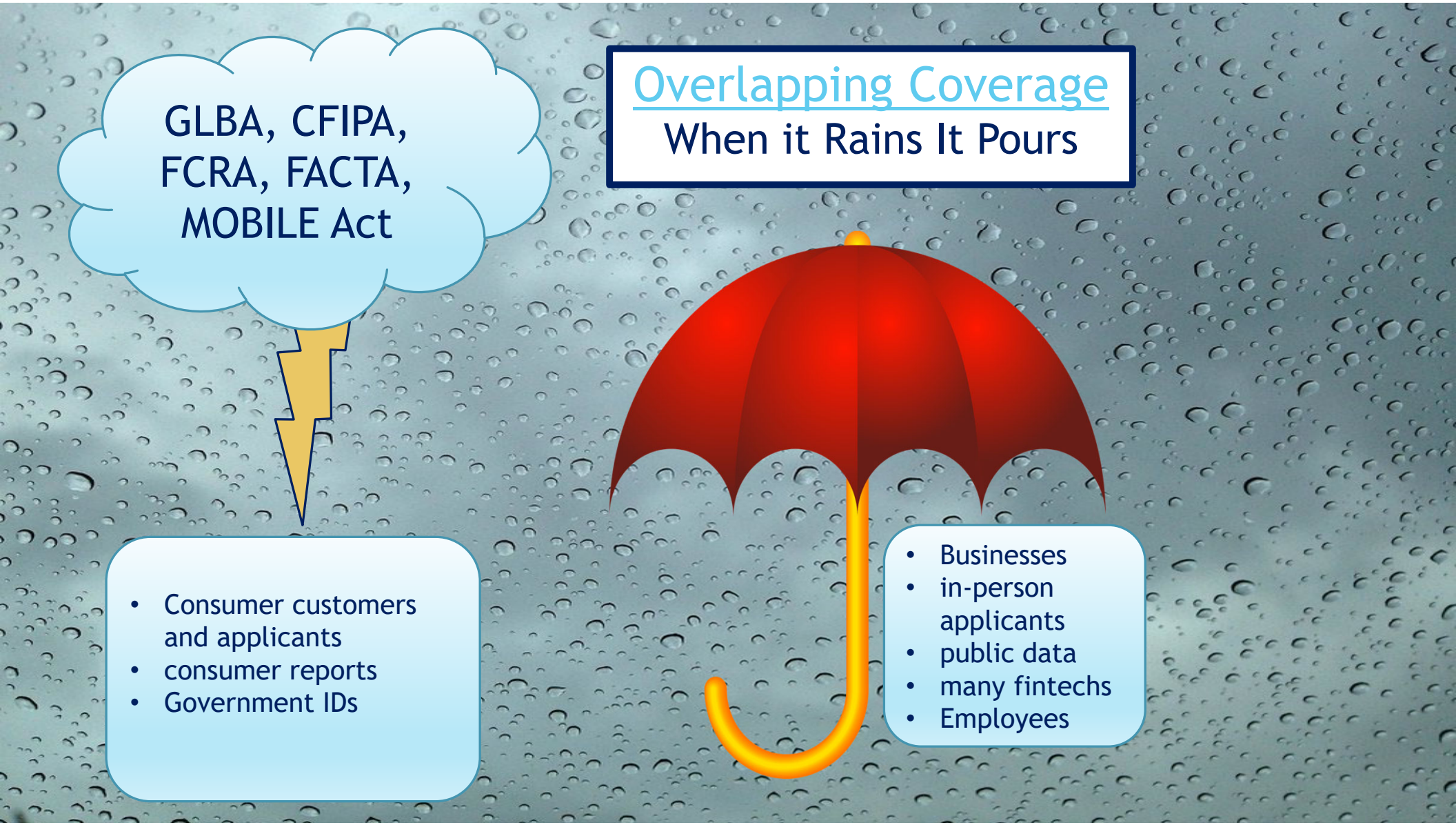
The Expanding Landscape of Financial Services Privacy – CPRA and Beyond

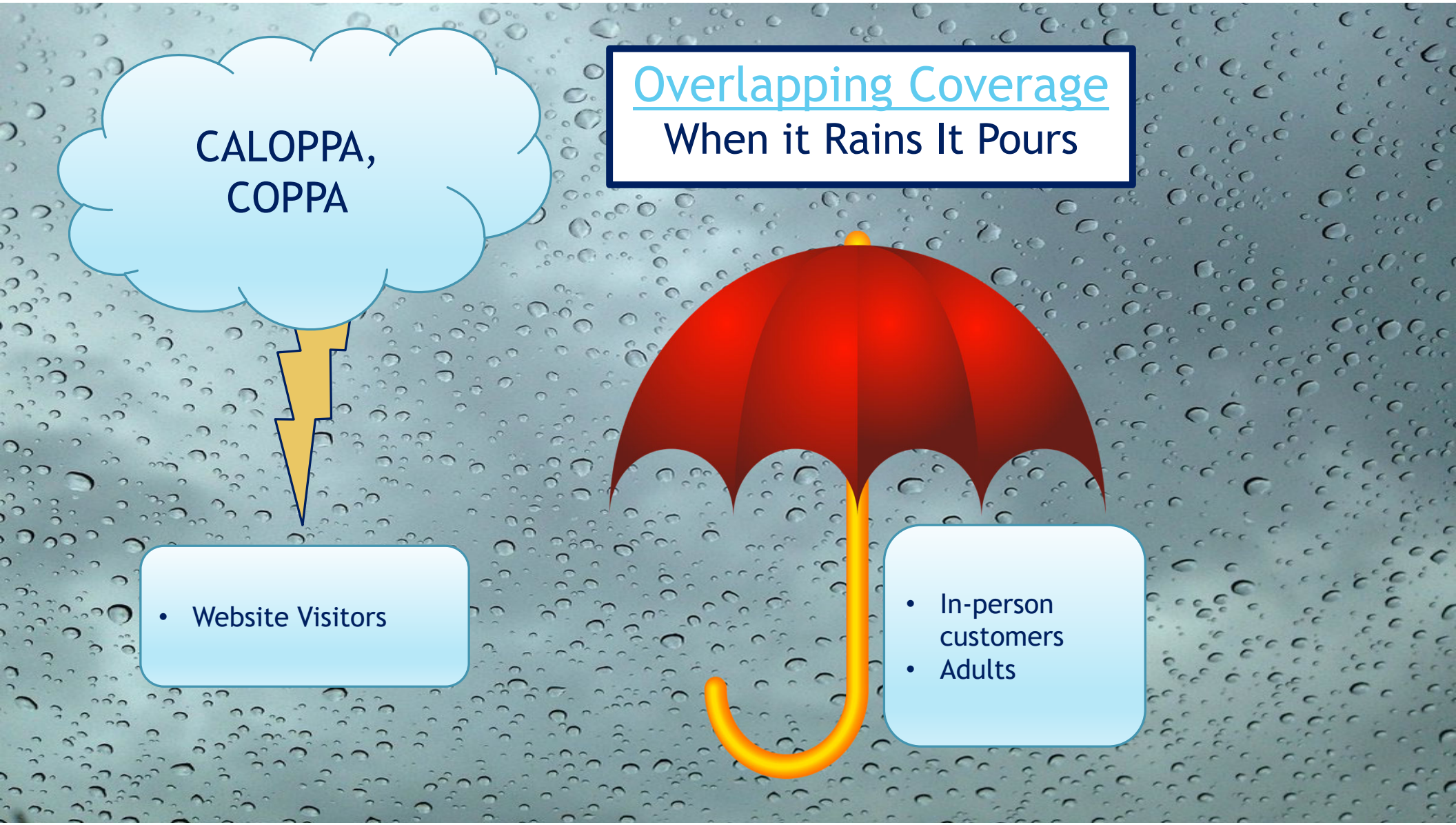
September 13, 2023

Paul Shimotake, Senior Counsel – Wells Fargo
Sheri Porath Rockwell, Counsel – Sidley Austin LLP
Nick Adams, US Chief Privacy Officer – BMO Bank N.A.

Legal Sources of Privacy Protection in the Financial Industry

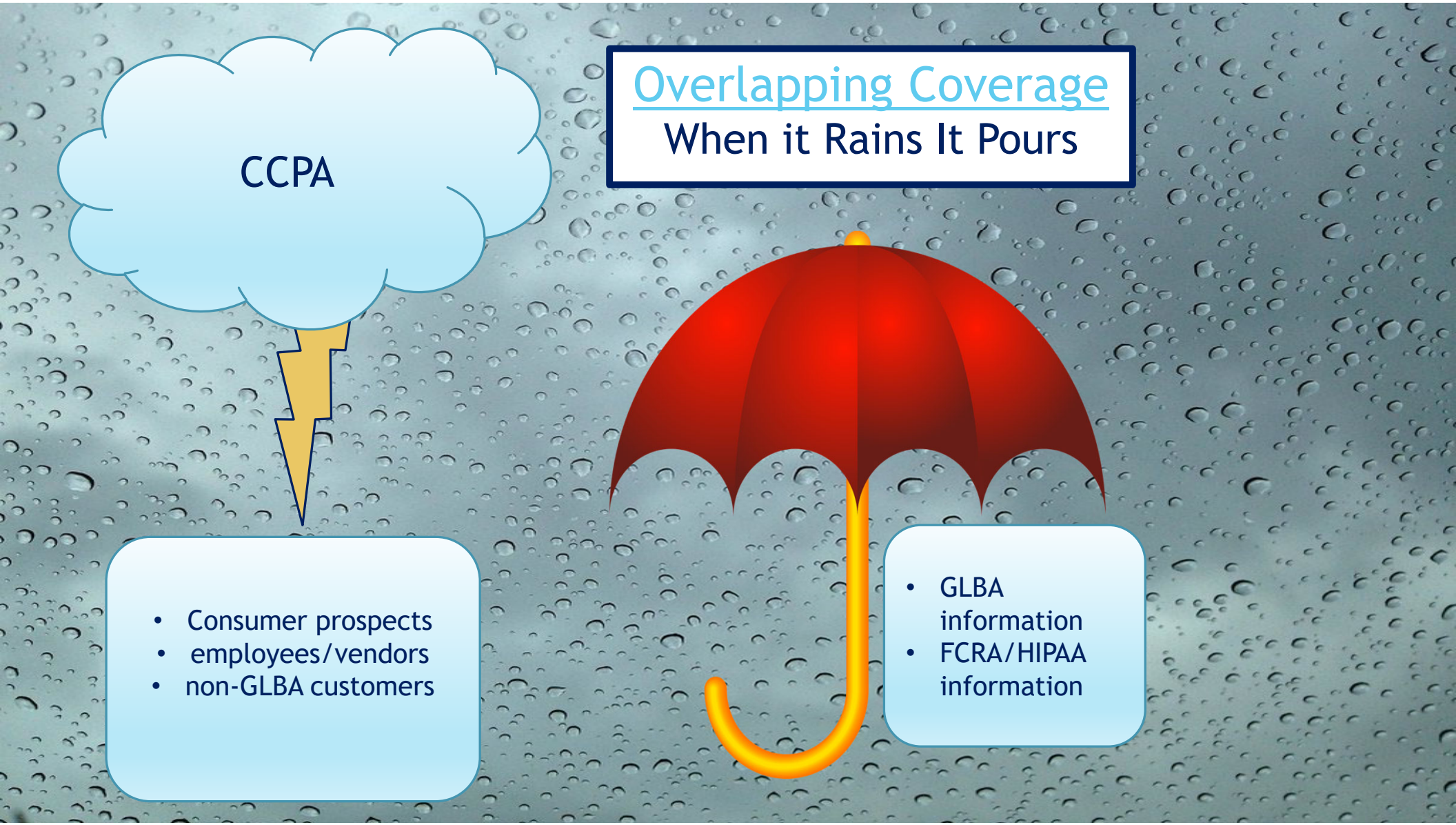



Overlapping Coverage
When it Rains It Pours
GLBA, CFIPA, FCRA, FACTA, MOBILE Act
• Consumer customers and applicants
• consumer reports
• Government IDs
• Businesses
• in-person applicants
• public data
• many fintechs
• Employees


Overlapping Coverage
When it Rains It Pours
CALOPPA,
COPPA
• Website Visitors
• In-person customers
• Adults

Overlapping Coverage

When it Rains It Pours

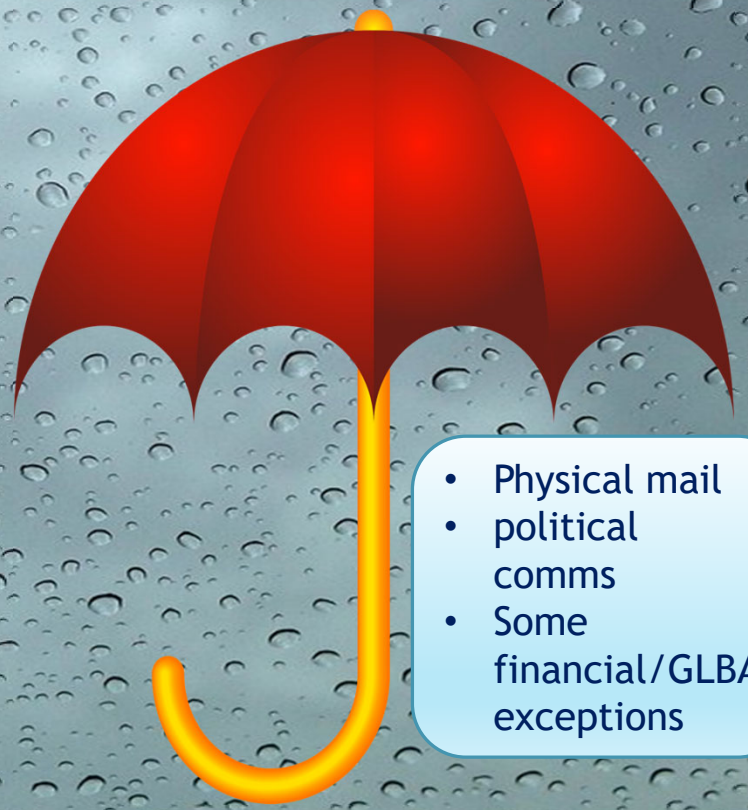


Overlapping Coverage

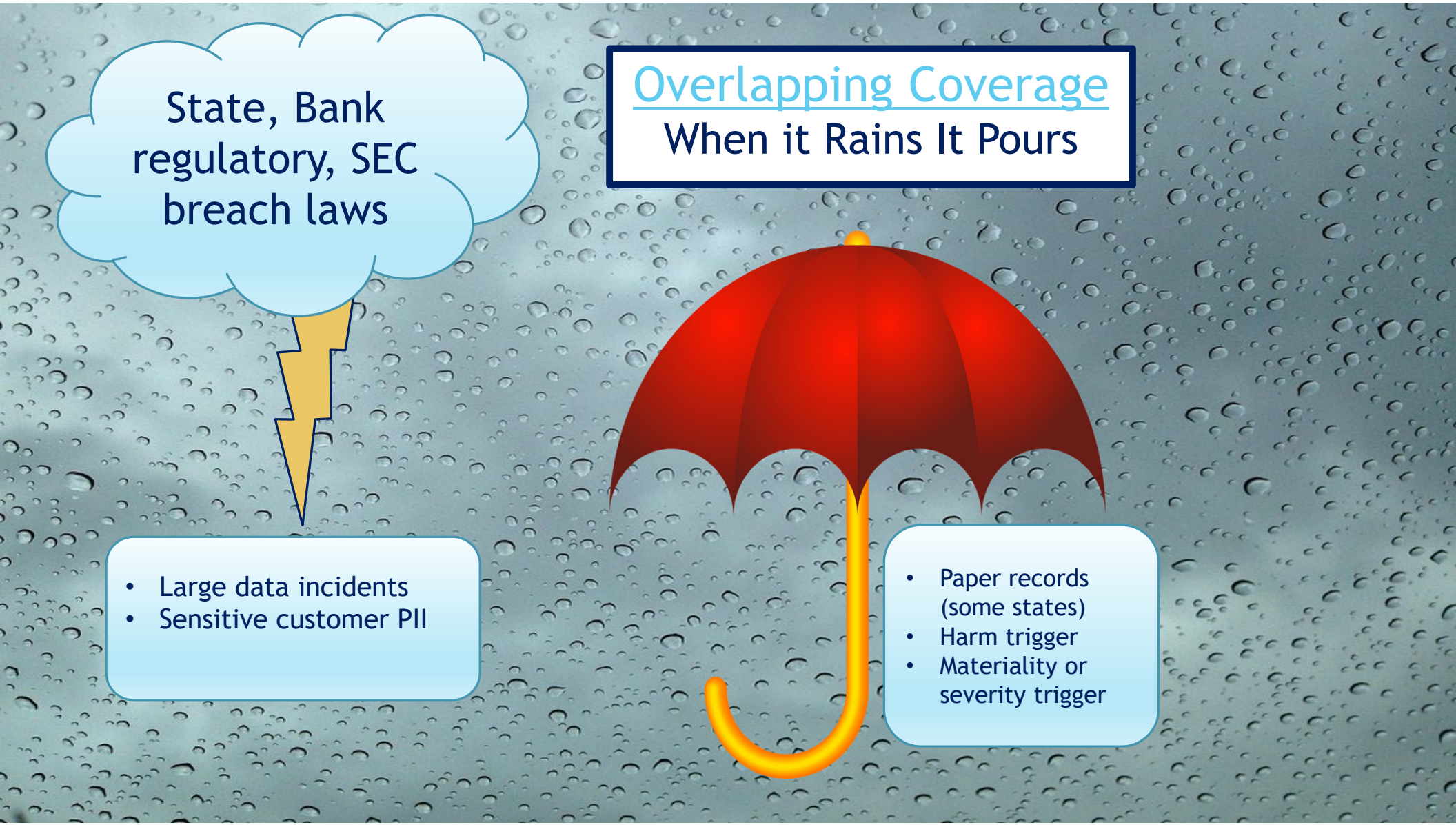
When it Rains It Pours

TCPA, CAN SPAM, Biometric, Wiretapping

- Customers and prospects
  - non-GLBA or non-financial entities



- Physical mail
- political comms
- Some financial/GLBA exceptions


State, Bank regulatory, SEC breach laws
Overlapping Coverage
When it Rains It Pours
• Large data incidents
• Sensitive customer PII
• Paper records (some states)
• Harm trigger
• Materiality or severity trigger

Battle Lines for Federal Legislation

- Exceptions
  - GLBA entity-level vs. information-level
    - Scope of GLBA interacting with state exemptions
  - B2B and employee coverage
  - Other federal laws (HIPAA, FCRA/FACTA, COPPA)
- Preemption
  - Strong field preemption vs. narrow direct conflict preemption
  - Sunrise or sunset provision
  - Floor vs. ceiling approach
- Private Right of Action
  - All provisions vs. data breach only (i.e. CCPA)
- Enforcement
  - FTC, CFPB, banking regulators

2023 Near Misses

- 15 states had failed privacy legislation in 2023
  - 12 states have enacted consumer privacy legislation
  - 6 states still have active legislation
- McHenry released discussion draft of GLBA amendment bill in 2022, passed House Financial Services Committee in February – faces CPPA opposition
- What is preventing federal action?
  - Genuine policy disagreements (preemption, enforcement)
  - General political intransigence
  - Shiny objects problem (AI, crypto)
  - Ever-increasing state action (perception of the problem)
- What could spur federal action?
  - Bipartisan animosity towards big tech
  - Another Cambridge Analytica
  - Politically sensitive use of banking data by law enforcement

CCPA/CPRA Developments

- Regulations on Right to Correct, Third Party Collection, Sensitive Personal Information, Right to Limit finalized in March, currently stayed until March 2024 by Chamber of Commerce litigation, appeal expected
  - New rights, sunset of B2B and employee exemptions granted by statute, not delayed
  - Agency has indicated enforcement priorities include employee rights fulfillment (employee disclosures pre-existed), disclosures
  - Already focus on data "sales," opt-outs, and GPC implementation
  - Draft regulations covering cybersecurity audits and risk assessments presented to Agency Board on Sept. 8, automated decision-making to follow

Key Enterprise Data Management Questions

*Ultimately, the CCPA and similar laws will require companies to answer **five important questions** concerning its data. A company's ability to answer all five of these questions for **all** of its data is critical to compliance with existing and emerging privacy laws:*

Potential Blind Spots for Banks

- Cookies and pixel tags – understanding what data is being transmitted, whether it is identifiable personal information, and whether it could qualify as sharing/selling.
  - Retargeting cookies as "sharing" debate is over according to the CPPA
- Customer and employee rewards programs – are they "financial incentive" programs?
- Expanding services into HIPAA-covered or "health data" territory
- Old statutes applied to new technology (CIPA, VPPA)
- Use of generative AI
- Employee CCPA compliance
- Financial privacy as byproduct of other political battles (state MCC bills, medical/reproductive health bills)

Key Operational Takeaways

- Data quality, tagging, and building in controls and places for consent/disclosure during product and infrastructure development has never been more important
  - Otherwise risk having to scrap projects already built to comply with new laws/regs
- Increasingly hard to treat privacy compliance on a per-law or per-regulation basis; banks should have overarching policies and strategies that address most privacy rights for most customers and employees, and align with key privacy principles
- Ensure that executive leaders and the Board of Directors have a thorough understanding of the evolving privacy landscape, and how it impacts existing and future business
- Prioritize benchmarking with your peers
- Trust but verify – ensure that you have proper assurance (monitoring, testing, audit) around privacy activities. If you don't detect gaps, others will do it for you.
- Play as a team – issue spotting can't be exclusively centralized, need privacy advocates throughout the organization.
- Vendor management – privacy is now as important as data security

Privacy Enforcement and Litigation Trends

- VPPA cases
- CPPA employee investigative letters
- CIPA lawsuits against banks, voice identification providers
- Agency targeting companies that do not allow consumers to efficiently exercise their rights
- Ad tech opt outs and opt in
- Launch of CPPA complaint portal
- Data breach class action trends

Q&A