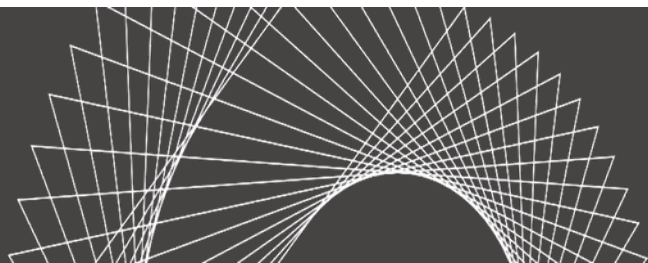


The Evolving Privacy and Cyber Policy Landscape



Akin Gump
STRAUSS HAUER & FELD LLP

Association of Corporate Counsel – Santa Clara, June 6, 2019

Hyongsoon Kim, Partner Akin Gump Strauss Hauer & Feld LLP

Natasha Kohne, Partner Akin Gump Strauss Hauer & Feld LLP

Michael Stortz, Partner Akin Gump Strauss Hauer & Feld LLP

Overview of Federal and State Policy Landscape

A Situation in Flux



Current Federal Regulations

Alphabet soup of federal regulators



Regulations are typically industry or topic specific

Health Sector
HIPAA, HITECH

Financial Servs.
GLBA

Gov. Contracts
DFARs

Specialized regulations have given rise to specialized litigation

VPPA

TCPA

FCRA

COPPA

Legislative Developments Pushing New State and Federal Privacy Proposals



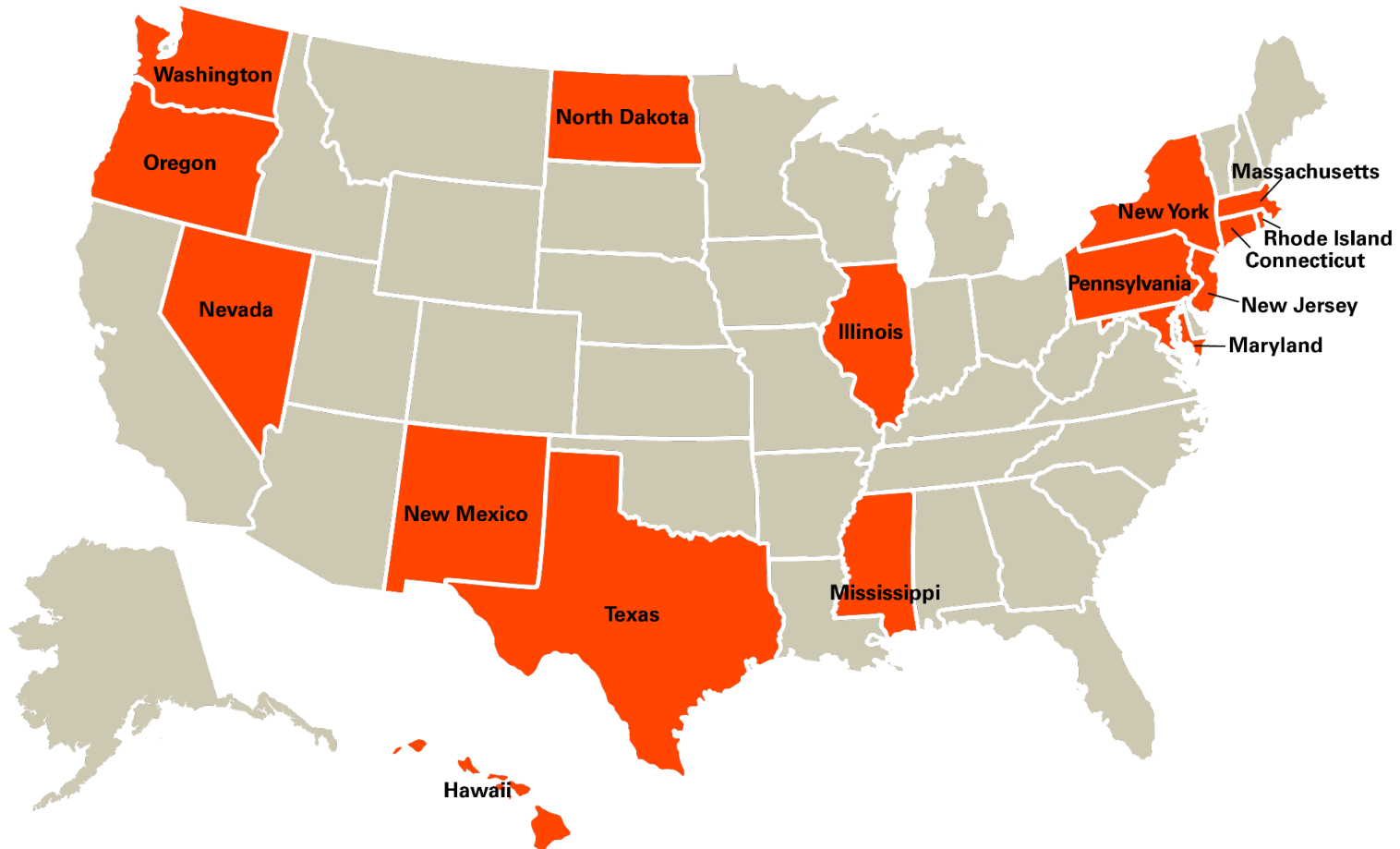
The 2018 California Consumer Privacy Act



The EU General Data Protection Regulation

Other States Have Followed California's Lead

States have followed California, with 17 states introducing CCPA-similar privacy bills in 2019:



Key Facts About Introduced State Legislation

Of the 10 pieces of active pending legislation similar to the CCPA:

4 of 10

Consumer
Private Right of
Action

3 of 10

Exemptions of
information
covered by
HIPAA

2 of 10

Exemption for
information
covered by GLBA

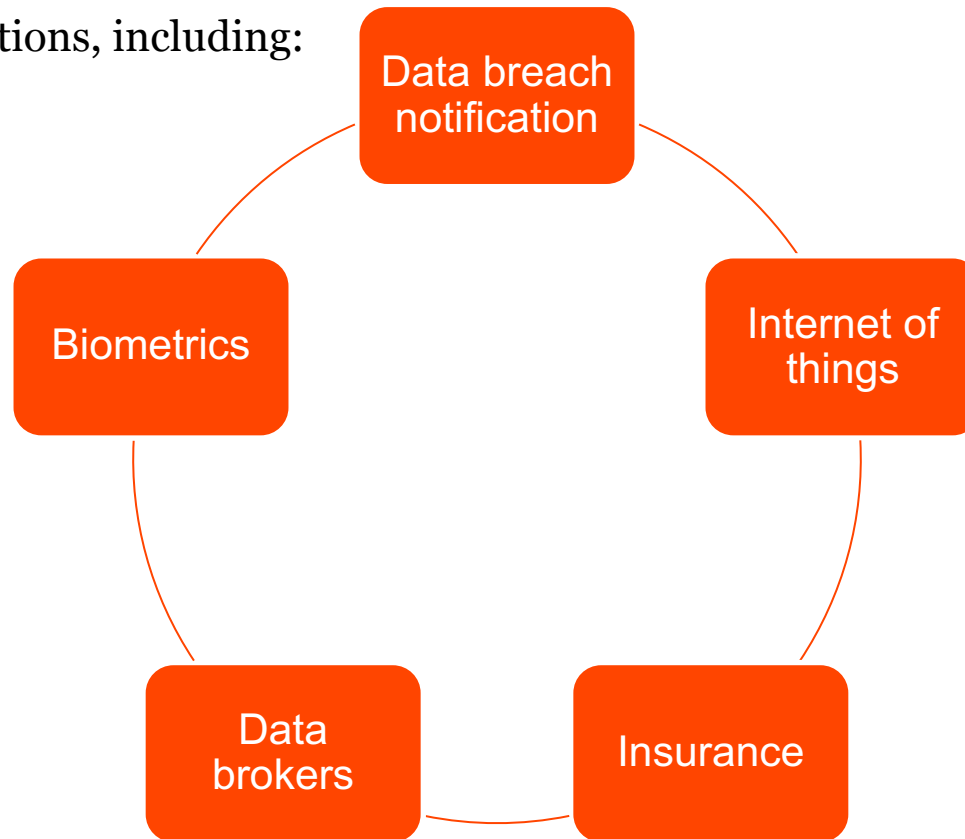
4 of 10

Inferences in
definition of
personal
information

Additionally, New York has a separate, pending Private Right of Action bill that would establish a PRA in the event a breach of consumer's identifying information

State Law Regulation - Overview

- In 2018, at least 35 states introduced more than [265 bills](#) or resolutions related to cybersecurity
- Wide variety of regulations, including:



Other Key State Laws



California's IoT law requires connected devices to have “reasonable security” (e.g., unique passwords, new authentication before first time access, etc.).



Maine has a law that is currently before the Governor that would bar internet providers from using or selling consumer browsing history and other data without first getting consent.



Ohio's law provides a safe harbor for data breach claims for companies that adopt administrative, technical, and physical safeguards to protect against breach.

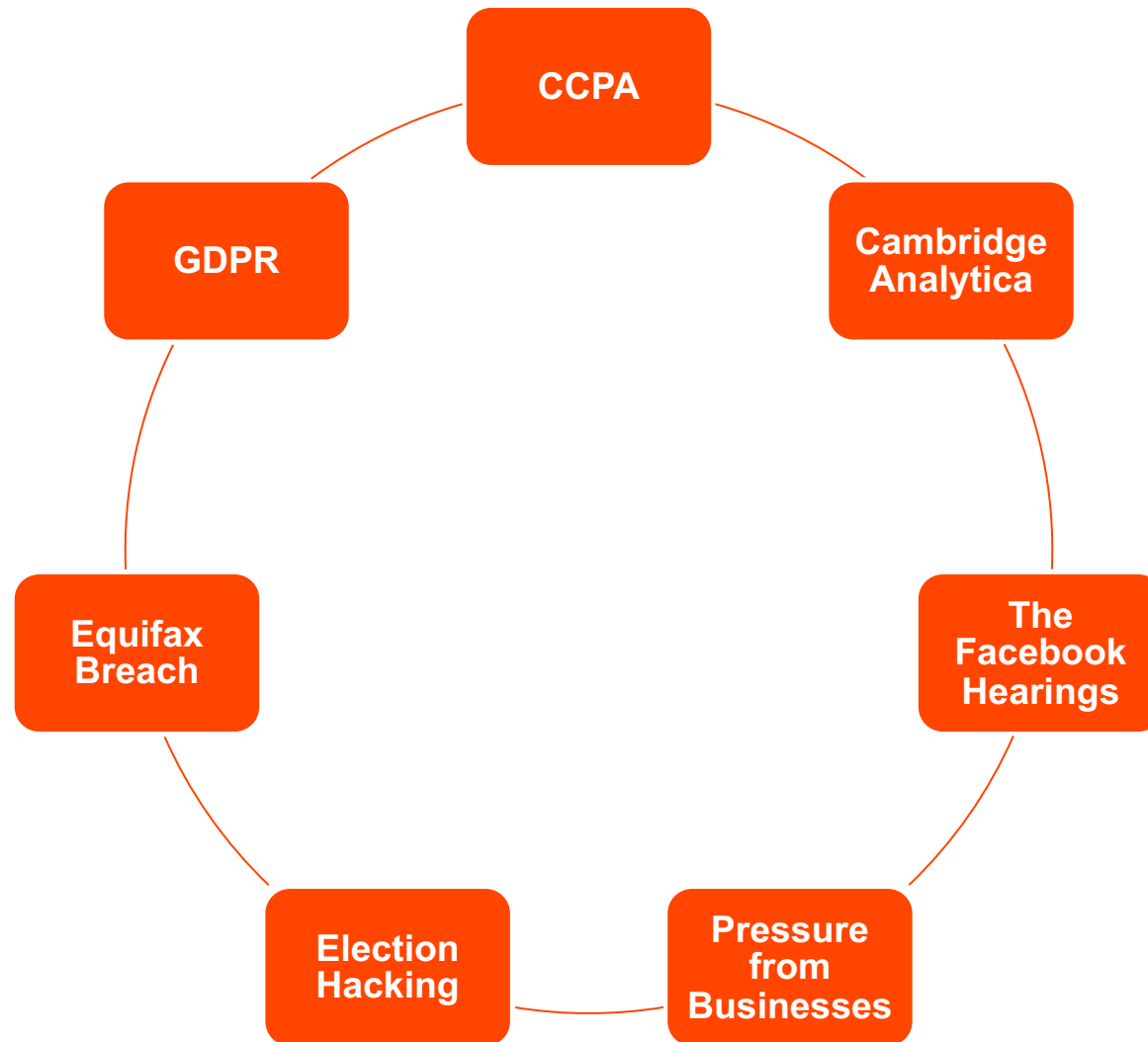


Vermont's data broker regulation requiring registration, reporting, and security controls took effect on January 1, 2019.

What About a Federal Fix?

- Possibility of federal legislation passing increased, not because of shift in control in Congress, but due to CCPA's 2020 effective date
- 39 proposed or pending federal bills
 - 20 privacy
 - 11 data security / breach notification
 - 8 other remedial measures related to privacy / security
- Senate Commerce privacy working group leading charge; promised draft legislation earlier this year, now suggesting before August recess
- Big push for legislation to preempt CCPA; CA representatives oppose

Triggers for Federal Action on Privacy



Common Threads of Federal Proposals

- Preemption
- Disclosures regarding data collection, usage, and dissemination
- Data subject rights
- Breach notification
- Clear privacy policies
- Duty of care
- Unlikely to be prescriptive on cybersecurity

Regardless of proposals, there is likely to be increased enforcement by all agencies (e.g., FTC inquiry into mobile carriers, SEC inquiry into BEC)

The FTC Commissioner has specifically asked for civil penalty authority and some Administrative Procedures Act rulemaking authority

Regulation Proposals are Raising Risk and Liability


Sen. Warren has called on Congress to pass legislation that would include jail time for corporate executives found liable for a data breach or other privacy violations. Sen. Wyden has also proposed legislation that would impose criminal charges for privacy violations.



Sen. Klobuchar has said: “If they’re making money off of you, you should make money off of them. So if they start sharing your data in a big way, we should start taxing them for that and that money should go back to consumers.”



Sen. Warner supports, among other things, adoption of an “information fiduciary” system whereby service providers assume special duties to respect and protect information they obtain.



Sen. Kennedy and others have proposed legislation that would transfer back to consumers the ownership rights for any content they created and posted to social media sites.

Possibility of A Federal Private Right of Action?

Split Parties - Dem. Members of Congress pushing for a PRA; Republicans oppose.

- Sen. Thune (R-SD): “The Democrats have a real interest in . . . a private right of action. Republicans have differing views.”

Senate

- Sen. Blumenthal (D-CT): “I think a private right of action generally upholds individual rights. ***We ought to be seriously considering it.***”
- Sen. Moran (R-KS) questioned witnesses about concerns associated with PRA in March.
- Sen. Coons (D-DE) inquired about benefits of the CCPA’s PRA during a hearing.

House

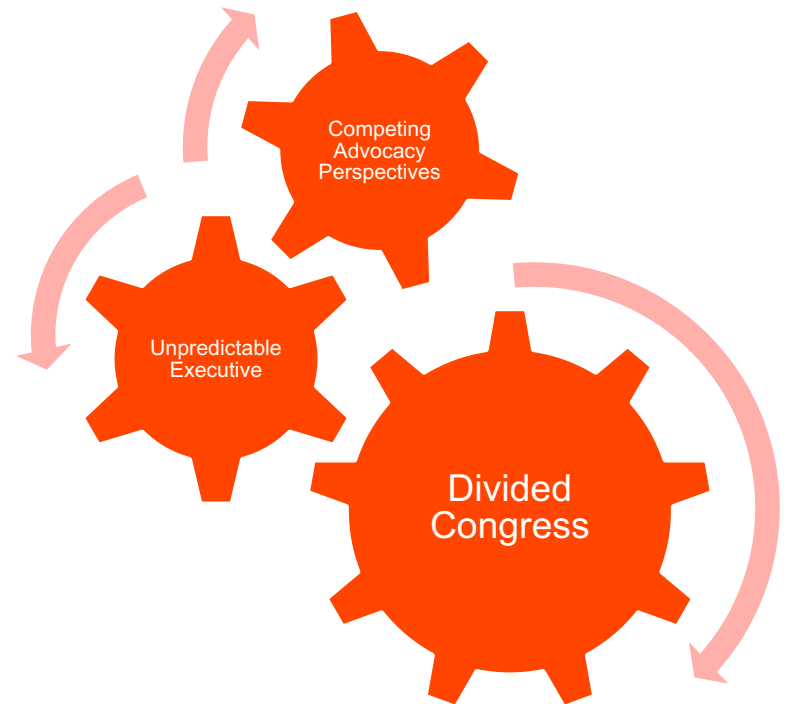
- Rep. Walden (R-OR) raised concerns about a private right of action, stating, “I don’t want to end up creating a platform that looks a lot like patent trolls.”
- Rep. Carter (R-GA): “And certainly, ***we don’t need plaintiffs’ attorneys to be involved in this***, we need the FTC to be the cop on the beat as you described them.”

California’s Influence

- California Attorney General Becerra, an advocate for a private right of action on the state level, has met with Sen. Cantwell (D-WA) to discuss components of federal legislation.

Significant Uncertainty Remains

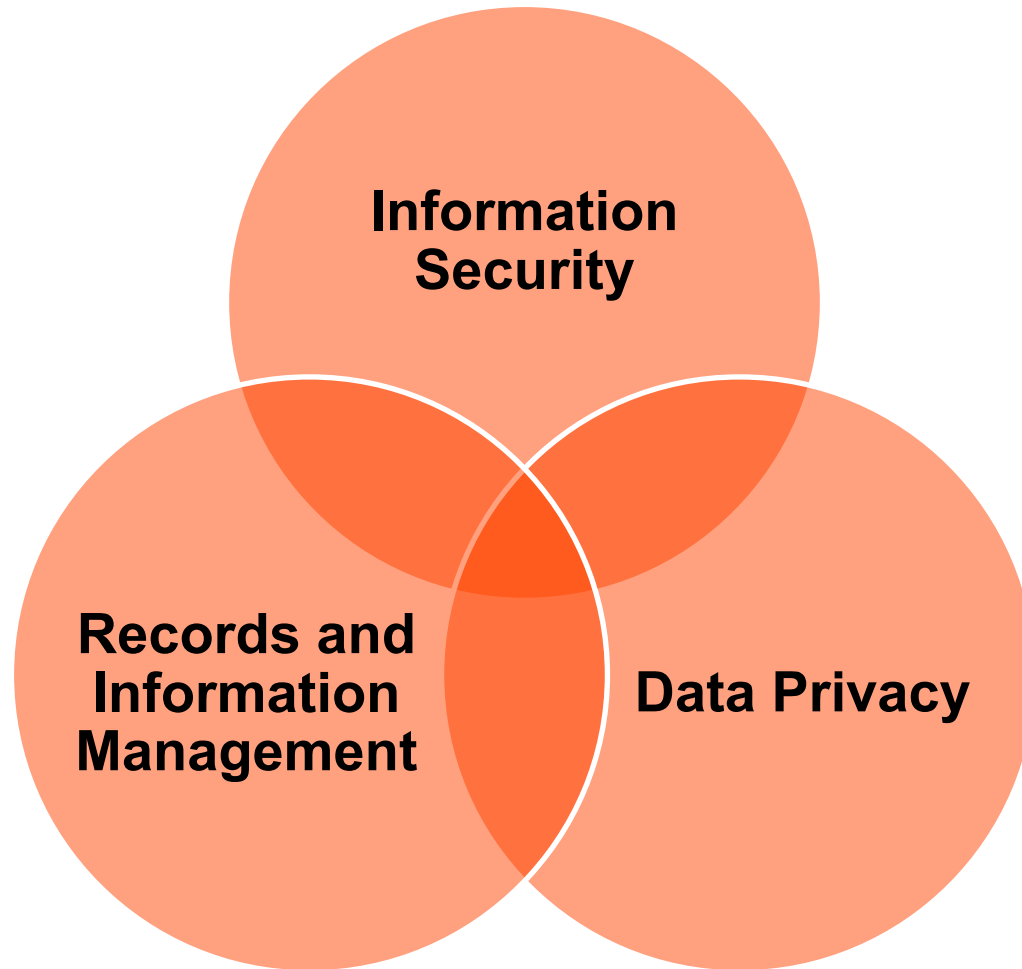
- Congressional approaches vary
 - House vs. Senate
 - Committee hearings
 - Looming 2020 race
- Motivated advocacy pushing agenda
 - Industry advocates vs. consumer activists
 - State regulators pushing their own role
 - Federal preemption key issue
- Position of Executive Branch is unclear



Tactics to Combat Privacy and Cyber Claims

What Every Company Should Consider *Before* Being Served

Information Governance



Information Governance – Risk Mitigation

- Understand what you have, where it comes from, where it is stored, and who has access.
- Collect and keep only what you need.
- Encrypt your data at rest and in transit.
- Ensure Board and management oversight.
- Train your employees.
- Understand your vendor risk and require more security from vendors.
- Implement practical policies.
- Anonymize and deidentify information.

Data Mapping
& Auditing

Minimization &
Retention

Vendor Risk &
Access

Encryption/
Redaction

Anonymization

Policies &
Procedures

Employee
Training &
Testing

Board
Oversight

What Regulators Consider Reasonable Security Practices – FTC Perspective as Overview

Through multiple FTC cases, we have a general sense of what the FTC considers “reasonable security” – or the *minimum* requirements a company must meet. These points are often reflected in guidance from other regulators.

Administrative Measures:

- Information security program
- Incident response plan
- Training
- Storing data (disposing unnecessary information)
- No unauthorized applications
- Responding to security warnings
- Monitoring and logging of activity

Technical Measures:

- Must use at least simple, low-cost defenses
- Credentials
- Secure access
- Encryption
- Cybersecurity software
- Monitoring
- Data disposal (electronic)
- Data loss prevention (electronic)

Physical Measures:

- Data disposal (physical)
- Physical security over data rooms and hard-copy data
- Data loss prevention (physical)
- Backup data access
- Disaster recovery

The CCPA and Other Laws Require Reasonable Security

- The CCPA mandates that businesses and service providers implement “reasonable security” controls, sufficient to comply with both the CCPA and the CA Data Breach Notification Law
- Consumers are permitted to bring a private right of action based, in part, on a business’s failure to implement reasonable security
- No CA law defines “reasonable security”
- In 2016, the CA Attorney General’s Office suggested that a company that complied with the 20 minimum security controls defined by the Center for Internet Security’s Critical Security Controls (“CIS Controls”) would meet this requirement
- It also suggested the failure to establish and document compliance with the CIS Controls would constitute a lack of reasonable security



Insight from Cases Examining Reasonable Security in California

- Plaintiffs have made it past the pleading stage where they alleged defendants failed to employ reasonable security by:
 - Failing to adopt industry-standard encryption, including on POS devices;
 - Failing to train employees;
 - Failing to sufficiently heed government warnings specific to industry;
 - Failing to promptly inform individuals of breaches although aware of breach;
 - Failing to adopt reasonable disaster plan and hampering recovery;
 - Failing to implement patches and address known cyber risks.

Key Takeaways

Encrypt
Information

Adequately
Train
Employees

Implement
Disaster Plans

Heed Security
Warnings

Adopt Data
Governance
Best Practices

Timely Disclose
Incidents/
Breaches

Attorney-Client Privilege and Work Product Protection – Overview in the Cyber Context



A/C Privilege – Communication (client and counsel) in which legal advice is sought or provided.

Work Product Protection – Materials prepared in anticipation of litigation.

- Steps should be taken as soon as an incident is suspected to try and ensure any investigation and related materials are protected.
 - Involve counsel immediately; incorporate outside counsel into your IRP.
 - Have counsel retain any forensic consultants or other resources used in investigation.
 - Ensure contracts with forensic team are clear about counsel leading engagement.
 - Have forensic team provide reports directly to outside lawyers.
 - Limit circulation of breach investigation materials to core group, keep high-level.
 - Anticipate that remediation materials and reports to Board may not be protected.
 - Limit disclosures related to investigation to facts alone.

Attorney-Client Privilege and Work Product Protection – Risk Assessments

Work Product Protection

Involve counsel in all communications

Counsel retains expert

Limit distribution

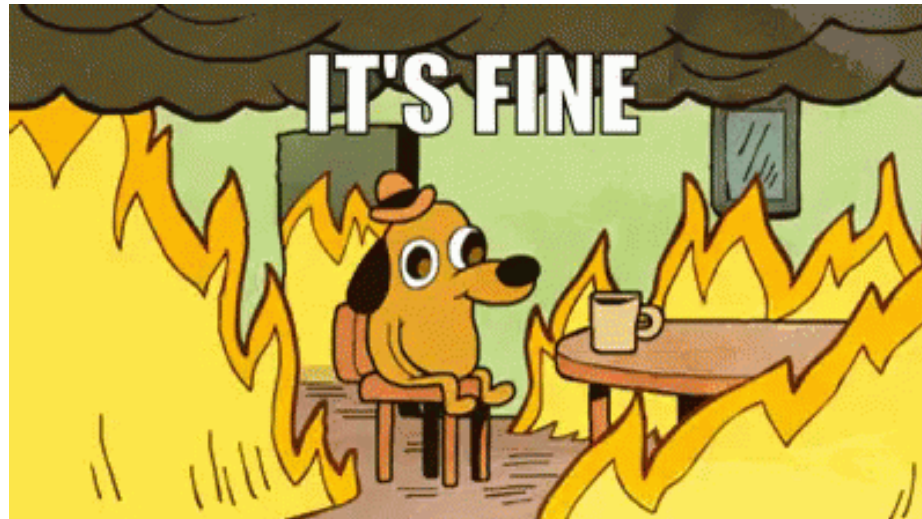
Results provided in counsel's report

Separate remediation

The Best Laid Plans . . .

Litigation is becoming increasingly common in the privacy context.

Defensible policies and practices are not enough, in-house legal should also have a sense of key litigation strategy issues before the company is sued.



Data Privacy Landscape – The Alphabet Soup

Key Privacy Statutes Relating to Litigation

Telephone Consumer Protection Act (TCPA)

Federal

Biometric Information Privacy Act (BIPA)

Illinois and counterparts (Washington; Texas – gov enforcement only)

Invasion of Privacy Act (CIPA)

California

Wiretap Act

Federal

Shine the Light Law (STLL)

California

Fair Credit Reporting Act (FCRA)

Federal

Children's Online Privacy Protection Act (COPPA)

Federal, with many states having similar laws

Video Privacy Protection Act (VPPA)

Federal

Song-Beverly Credit Card Act

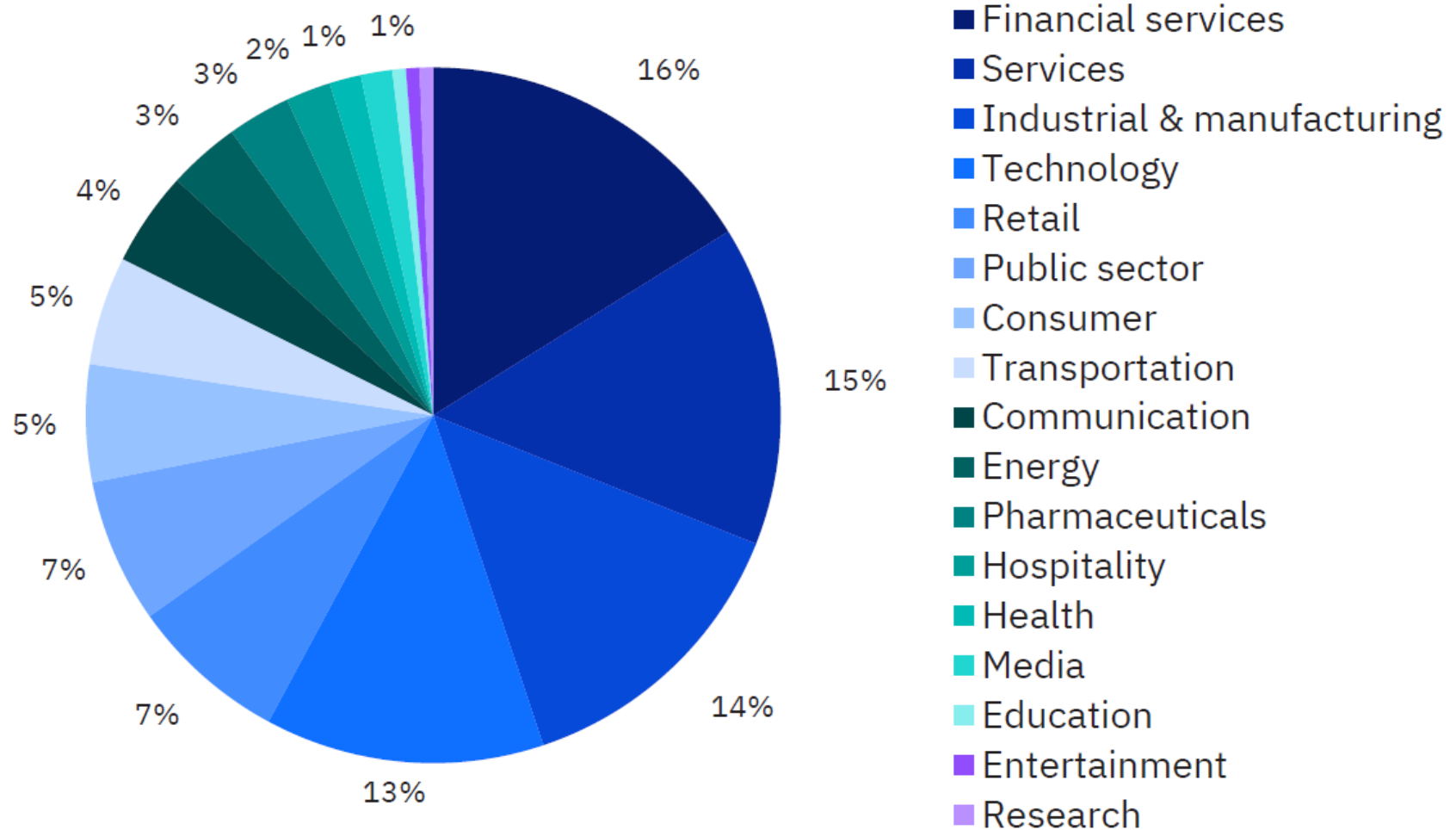
California and counterparts (Massachusetts)

California Consumer Privacy Act (CCPA)

California (Goes into effect Jan. 1, 2020)

Data Breach Risks – Industries Affected

Hackers target many different industries



Data Breach Risks – Industries Affected

- In the first half of 2019, there have been well over 100 data breaches made public
- The FBI estimates that only 10-12% of cybercrimes are actually reported
- Analysts estimate that less than half of companies globally are sufficiently prepared for a cybersecurity attack



- Popular and emerging recent targets for hackers include:
 - Cloud-hosted entities
 - Health/medical centers
 - e-Commerce retail
 - Crypto currency-based entities

Data Breach Risks – Information Types Exposed

- Hackers target sensitive data, including:
 - Full payment card details
 - User names
 - Social security numbers
 - Bank account numbers
 - Email addresses
 - Phone numbers
 - Encrypted passwords
 - Password hints
 - IP addresses
 - Personal health information



Data Breach Risks – Lawsuits Usually Follow Announcement of a Breach

- Individual damages may be small, but when claims are aggregated as a class action, overall liability can be significant
- Example: late last year, Marriot announced breach affecting 500 million customers
 - Multiple class action complaints filed within hours
 - One plaintiff sought \$25 per person, totaling a demand of \$12.5 billion
- Companies that have recently settled data breach class actions include:

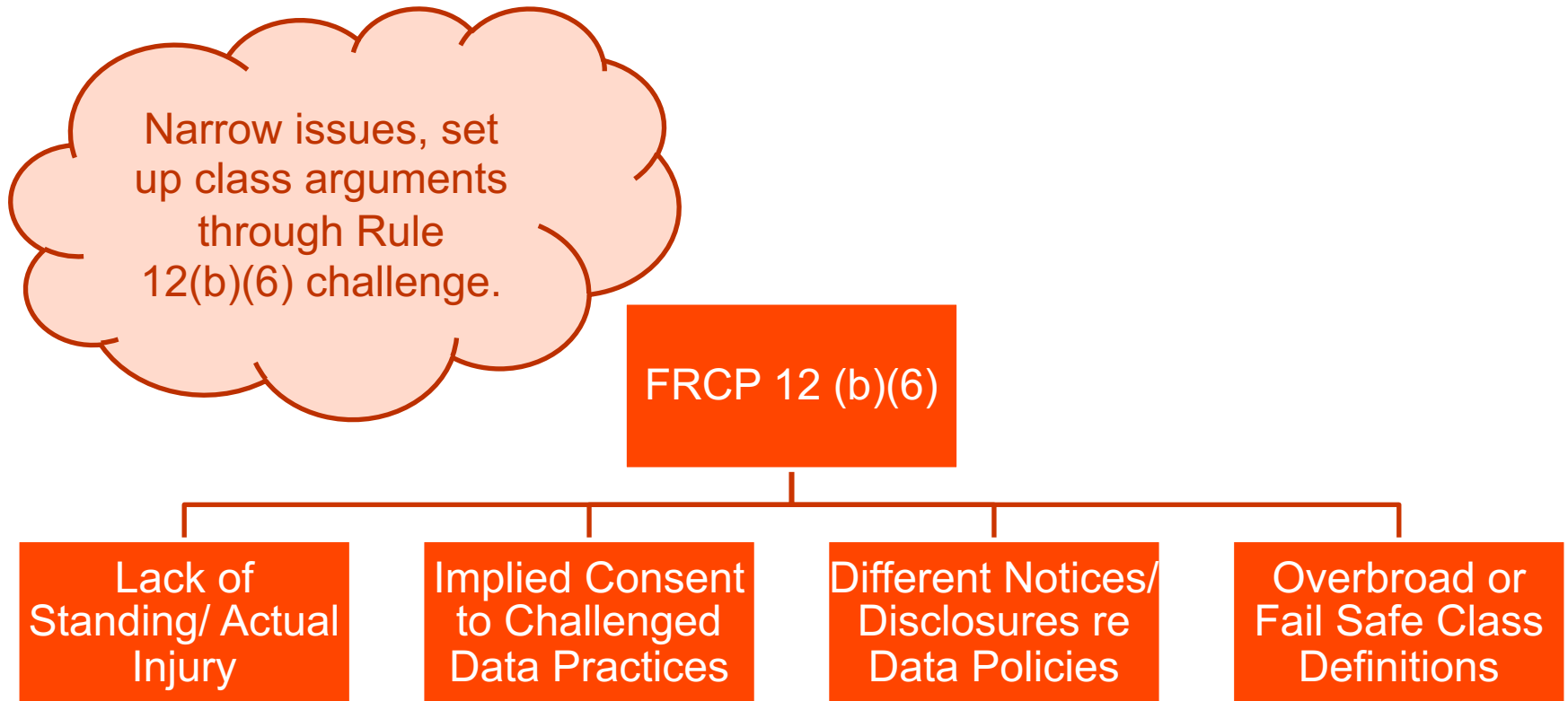


Standing – Recent Developments

- On March 20, 2019, in *Frank v. Gaos*, the Supreme Court vacated a Ninth Circuit privacy settlement in view of its 2016 *Spokeo* decision
- The Court reiterated that a plaintiff does not “automatically” have standing by claiming a violation of a statutory right that authorizes private action
- The post-*Spokeo* dust has not yet settled:
 - “Third Circuit: FACTA Class Plaintiff Lacked Concrete Injury Required for Standing Under *Spokeo*”
 - “Second Circuit Joins Consensus Holding TCPA Plaintiffs Have Standing Under *Spokeo*”
 - “Ninth Circuit Rejects Standing for Plaintiffs Alleging Inaccurate Credit Reports, Relying on *Spokeo v. Robins*”
 - “11th Cir. Splits from Other Circuits on *Spokeo* Standing”
 - “8th Circuit Dismisses FCRA Claims for Lack of Standing”



Threshold Challenge to Complaint



Hurdles at Class Certification - Experts

Experts will likely drive battle at class certification;

What does this mean in practice?

- Plaintiffs will present **common proof of liability, class damages model** through expert report in support of class certification
- Certification may hinge on adequacy of both reports (*Hannaford*; *Nguyen*)
- Depositions, opposition experts key
- *Daubert* challenge at class certification



Hurdles at Class Certification – Prevailing Individual Issues

“No Injury” Class

Individual Issues
as to Consent

Varying
Disclosures to
Class Members
re Data Policies

No Common
Classwide
Damages

Rule 23(c)(4)
Issues Class

Arbitration and Class Action Waivers

- Proof of consent:
Clickwrap/browsewrap
- Enforceability in data privacy context
- Broad scope provision
- Opt out option
- Waiver of public injunctive relief
(*McGill*)

DISPUTES

Any dispute or claim relating in any way to your use of any [REDACTED] Service, or to any products or services sold or distributed by [REDACTED] or through [REDACTED].com will be resolved by binding arbitration, rather than in court, except that you may assert claims in small claims court if your claims qualify. The Federal Arbitration Act and federal arbitration law apply to this agreement.

There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages), and must follow the terms of these Conditions of Use as a court would.

To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to our registered agent [REDACTED]

[REDACTED] The arbitration will be conducted by the American Arbitration Association (AAA) under its rules, including the AAA's Supplementary Procedures for Consumer-Related Disputes. The AAA's rules are available at www.adr.org or by calling 1-800-778-7879. Payment of all filing, administration and arbitrator fees will be governed by the AAA's rules. We will reimburse those fees for claims totaling less than \$10,000 unless the arbitrator determines the claims are frivolous. Likewise, Amazon will not seek attorneys' fees and costs in arbitration unless the arbitrator determines the claims are frivolous. You may choose to have the arbitration conducted by telephone, based on written submissions, or in person in the county where you live or at another mutually agreed location.

We each agree that any dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated or representative action. If for any reason a claim proceeds in court rather than in arbitration we each waive any right to a jury trial. We also both agree that you may bring suit in court to enjoin infringement or other misuse of intellectual property rights.

Please view, print or save the documents linked below.

For more information on the main characteristics of the [REDACTED] service, please read our [Key Payment and Service Information](#).

☒ By clicking **Agree and Continue**, I hereby:

- Agree and consent to the [User Agreement](#), its policies, and the [Privacy Policy](#).
- Expressly instruct [REDACTED] to communicate specific information about me and my account to third parties in accordance with the Privacy Policy.
- Specifically and expressly consent to the use of website tracking methods, including cookies, and to the safe and secure transmission of your personal information outside the European Economic Area in accordance with the Privacy Policy.

User Agreement and Privacy Policy

These documents are designed to inform you of your rights and obligations when using the [REDACTED] service.

[Agree and Continue](#)

Competing Judicial Views of Privacy Claims

State law claims for intrusion upon seclusion require pleading that defendants' conduct occurred in a manner “highly offensive to a reasonable person.”

In data privacy cases, courts grapple with whether alleged data misuse meets this standard, in similar cases.

- *Manigault-Johnson v. Google* (D.S.C. March 31, 2019): capture of child's personal information and persistent identifiers on website and app did not state a claim.
- *McDonald v. Kiloo Apps* (N.D. Cal. May 22, 2019): capture of children's persona information through use of apps states a plausible claim for relief; reserving further determination until summary judgment.

Plausibility standard under *Twombly/Iqbal* in tension with “evolving societal norms.”

Questions?