Privacy and Data Security Forum: 2019 Year in Review and Preparing for 2020

Association of Corporate Counsel, National Capital Region – February 13, 2020

Natasha Kohne, Partner, Akin Gump

Michelle Reed, Partner, Akin Gump

Amy Yeung, General Counsel and Chief Privacy Officer, Lotame, Inc.

Moderated by: Anthony Pierce, Partner in Charge of Washington, D.C. office, Akin Gump

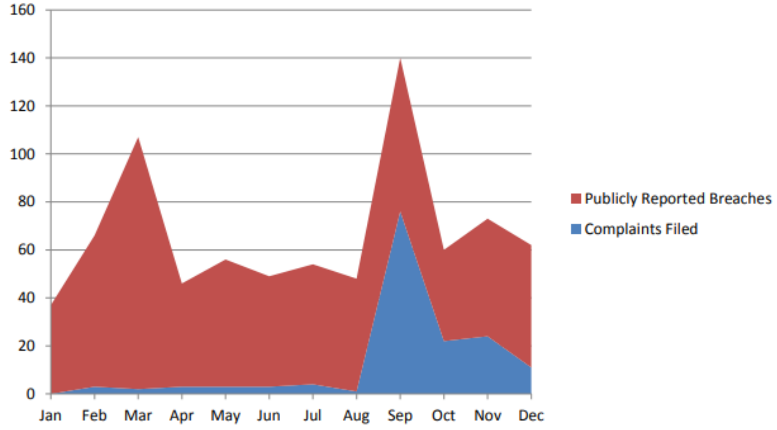
Data Breach Update and Outlook

Data Breach Litigation Trends – Number of Cases

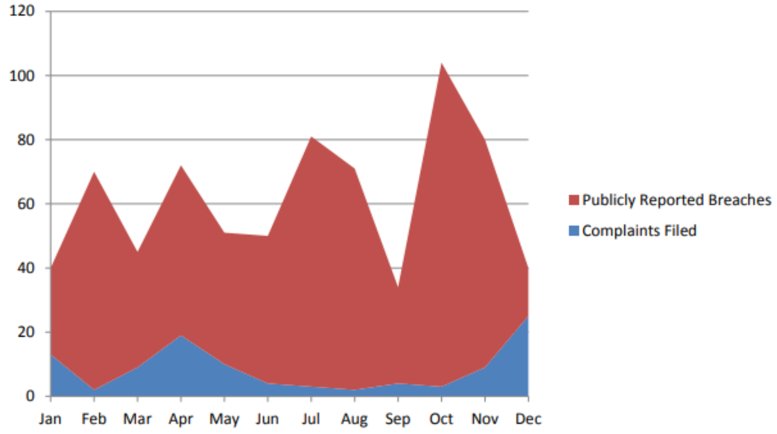
- **2017**
  - 152 complaints filed
  - Approximately 4.0% of data breaches publicly reported in 2017 led to class action litigation.
  - Slight increase from 2016, in which only 3.3% of publicly reported data breaches led to class action litigation relative to the number of breaches.

- **2018**
  - 103 complaints filed
  - 5.7% of data breaches publicly reported in 2018 led to class action litigation in 2018.
  - 1.7% increase from 2017 and a 2.4% increase from 2016, indicating a steady increase in class action litigation relative to the number of breaches.

The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during 2017.

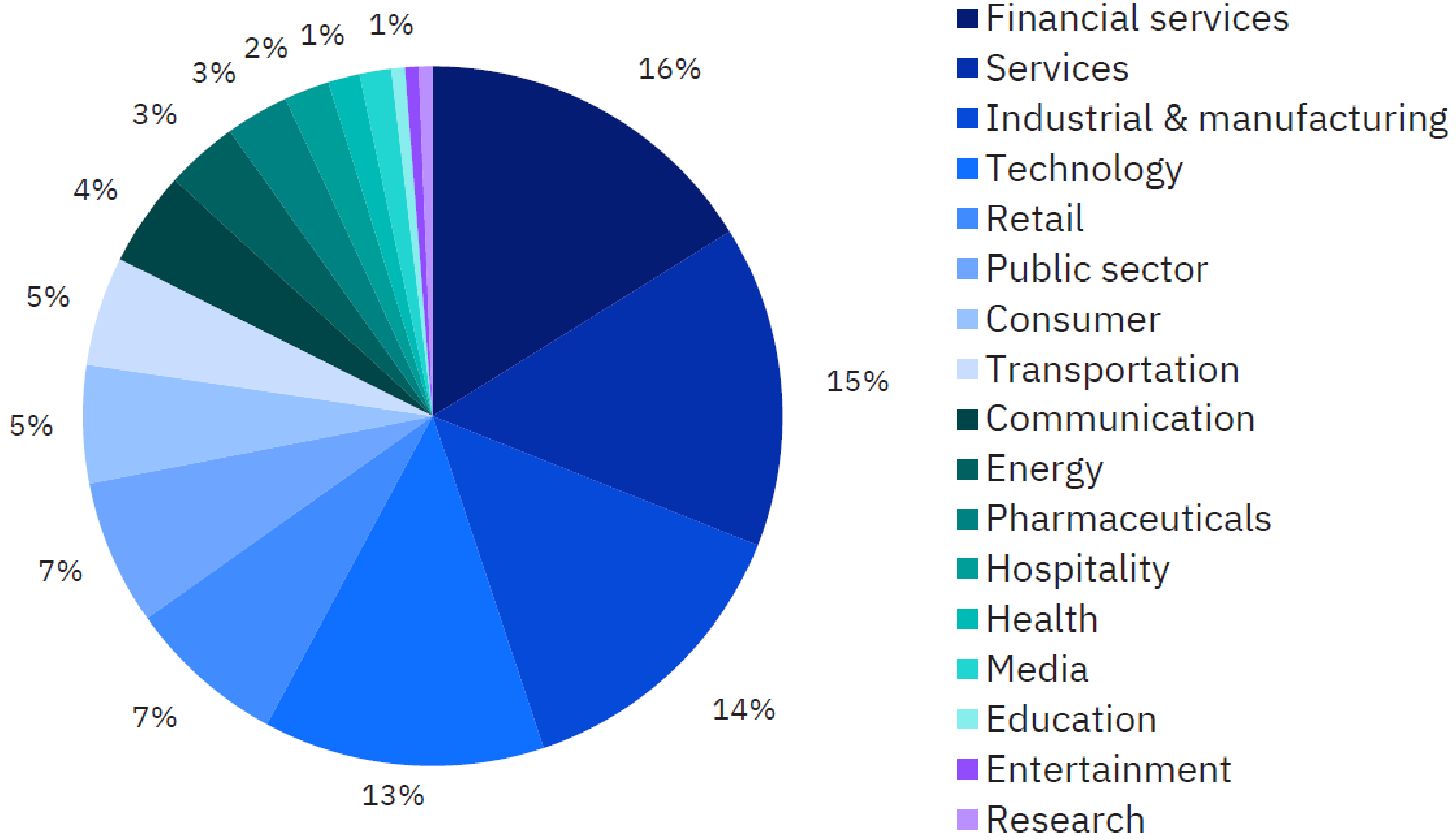


The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during 2018.

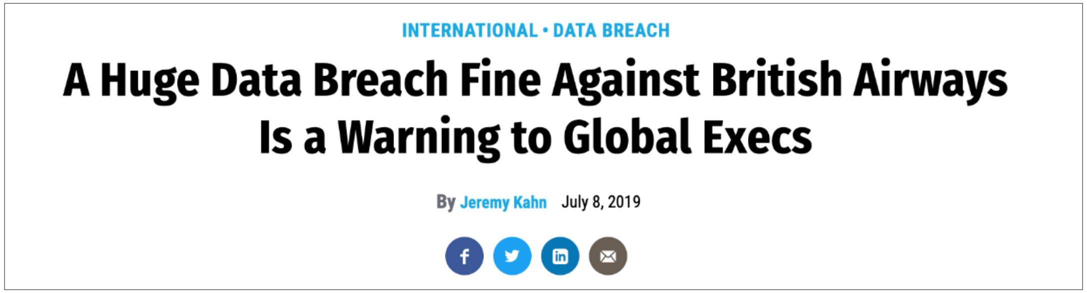


Data Breach Risks – Industries Affected

Hackers target many different industries



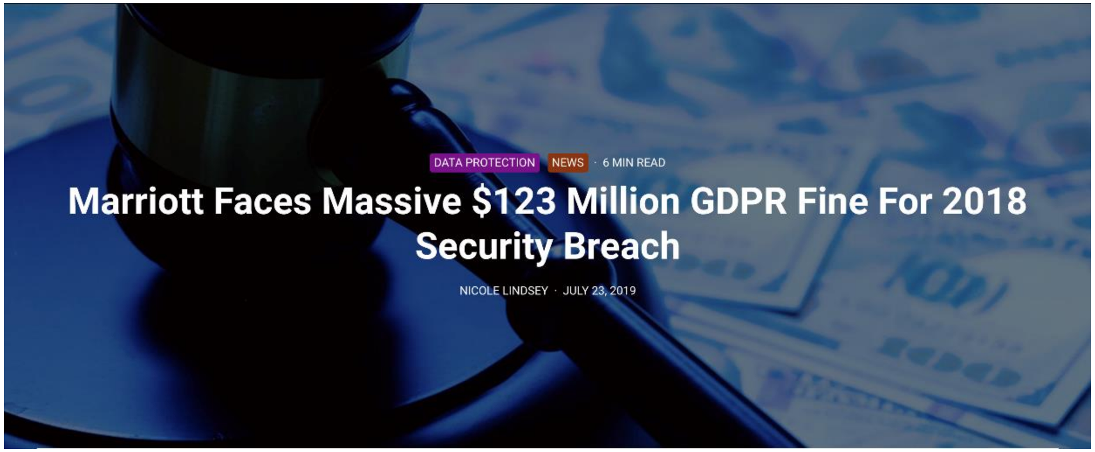
Massive Fines Are The New Normal?



INTERNATIONAL • DATA BREACH

A Huge Data Breach Fine Against British Airways Is a Warning to Global Execs

By Jeremy Kahn July 8, 2019



DATA PROTECTION NEWS · 6 MIN READ

Marriott Faces Massive $123 Million GDPR Fine For 2018 Security Breach

NICOLE LINDSEY · JULY 23, 2019

- The ICO announced fines for British Airways (~$230M) and Marriott (~$121M) for failure to maintain adequate data security and certain data protection failures.
- Among the largest fines we've seen in the EU; in BA case, high fine for the relatively small amount of individuals affected (~500k customers).

Equifax Data Breach

KEY POINTS

- ~147 million class members were offered:
  - a) Credit monitoring services for at least four years
  - b) Identity theft recovery services
  - c) Identity theft insurance up to $1 million
  - d) Reimbursement for resulting out-of-pocket costs
  - e) Six additional free credit reports from Equifax per year for seven years
- Equifax's additional obligations in the settlement:
  - a) $380.5 million in funding for class benefits, with up to $125 million in additional funding as needed
  - b) $1 billion investment in data security and technology enhancements
  - c) Independent audit of compliance
  - d) Judicial oversight and enforcement of audit compliance
  - e) Payment of more than $77 million in legal fees

SETTLEMENT ISSUES

- Data breaches nearly always include persons with exposed but not necessarily exploited information
- Equifax settlement process presented unique issues for addressing these class members

Cash Compensation Option

- Option of up to $125 in cash for persons who already had credit monitoring
- FTC said interest in this option was "overwhelming" and advised cash payment would be "nowhere near" that amount
- Current estimate is cash payment will be <$7
- All persons with actual out-of-pocket losses are expected to be fully compensated

Coordinated, Semi-Automated Objections

- 700+ "form" objections filed by 3rd party chatbot encouraging class members to object to settlement
- Court ruled these objections procedurally invalid
- Could we see more automated efforts like this?

Marriott Data Breach

KEY POINTS

- ~383 million affected individuals
- Compromised information includes names, home addresses, email addresses, phone numbers, DOB, loyalty account information and payment information
- Breach also includes millions of unencrypted passport numbers
- Multidistrict litigation in District of Maryland to oversee five tracks of litigation
  a) Consumer Class Action
  b) Financial Institution
  c) Securities Class Action
  d) Shareholder Derivative Action
  e) Government

LITIGATION ISSUES

- Marriott has moved to dismiss, arguing that there is no actual harm to the vast majority of affected individuals
- Court has ordered Marriott to produce copies of the forensic investigative report that details how the breach occurred
- Discovery stayed in securities and shareholder derivative suits due to PSLRA

CCPA Private Right of Action

Confidential – Not for Distribution Beyond Attendees

CCPA Private Right of Action

"(a) (1) Any consumer whose **nonencrypted and nonredacted personal information**, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an **unauthorized access and exfiltration, theft, or disclosure** *as a result of the business's violation of the duty to **implement and maintain reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information* may institute a civil action for any of the following:

> (a) To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident, whichever is **greater**;
>
> (b) Injunctive or declaratory relief;
>
> (c) Any other relief the court deems proper.

(Cal. Civ. Code § 1798.150(a)(1).)

Statutory Damages Assessment

In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to:

(a) the nature and seriousness of the misconduct,

(b) the number of violations,

(c) the persistence of the misconduct,

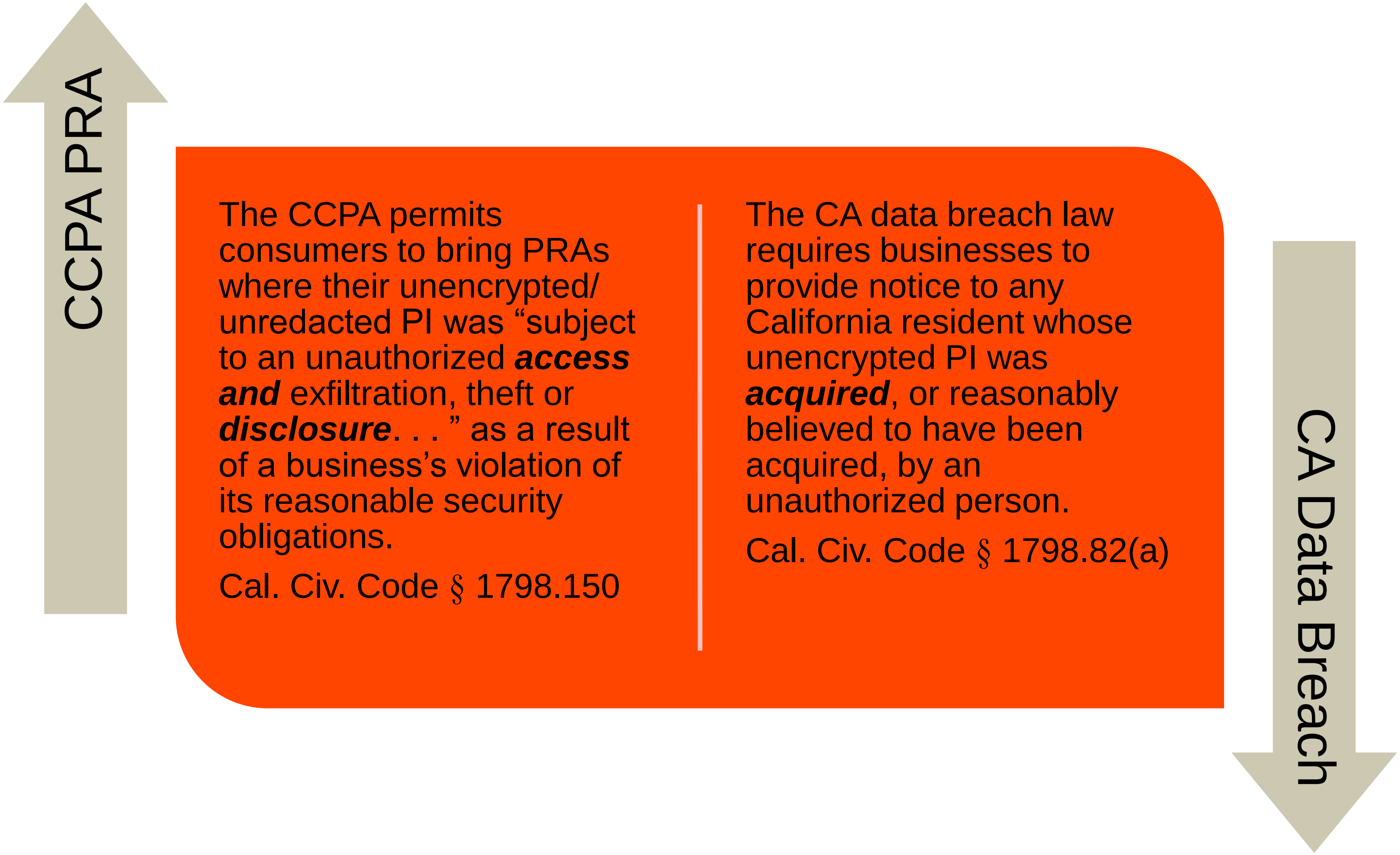
(d) the length of time over which the misconduct occurred,

(e) the willfulness of the defendant's misconduct, and

(f) the defendant's assets, liabilities, and net worth.

(Cal. Civ. Code § 1798.150(a)(2).)

Access Breach May Raise Risks



CCPA PRA

The CCPA permits consumers to bring PRAs where their unencrypted/ unredacted PI was “subject to an unauthorized ***access and*** exfiltration, theft or ***disclosure***. . . ” as a result of a business’s violation of its reasonable security obligations.

Cal. Civ. Code § 1798.150

The CA data breach law requires businesses to provide notice to any California resident whose unencrypted PI was ***acquired***, or reasonably believed to have been acquired, by an unauthorized person.

Cal. Civ. Code § 1798.82(a)

CA Data Breach

What Information Has to be Affected?

CCPA

““Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household..

“Personal information” does not include publicly available information. “Publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

CA Data Breach Law

“Personal information” means either of the following:

(A) An individual’s first name or first initial and last name in ***combination with any one or more of the following data elements,*** when either the name or the data elements are not encrypted or redacted:

- (i) Social security number.
- (ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
- (iii) Account number, or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual’s financial account.
- (iv) Medical information.
- (v) Health insurance information.
- (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

The Curious "Cure" Found in the CCPA

- CCPA requires consumers to give businesses 30 days' notice of a violation and an opportunity to address or "cure" the violation before they file suit.
- If the business cures the violation, the plaintiff cannot file a claim.

- "Cure" is not defined and no clear precedent on point.
- The CCPA also requires businesses provide consumers a written statement confirming that the violation(s) has been cured and that no further violations will occur.

NY SHIELD Act – A Reasonable Guide to Reasonable Security

Administrative Safeguards

- Designate one or more employees to coordinate the security program.
- Identify reasonably foreseeable internal and external risks.
- Assess the sufficiency of implemented safeguards to control identified risks.
- Train employees on the security program practices and procedures.
- Select service providers capable of maintaining appropriate safeguards and require those safeguards by contract.
- Adjust the security program in light of new business circumstances.

Technical Safeguards

- Assess risks in network and software design and in information processing, transmission and storage.
- Detect, prevent and respond to attacks or system failures.
- Regularly test and monitor the effectiveness of key features of the security program.

Physical Safeguards

- Assess risks associated with information storage and disposal.
- Detect, prevent and respond to intrusions.
- Protect against unauthorized access to or use of private information during or after collection, transportation or destruction of information.
- Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing any media so that the information cannot be read or reconstructed.

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
- Designate a qualified Employee
- Restrict Access
- Retain Service Providers
- No Unauthorized Applications
- Responding to Security Warnings
- Monitoring and Logging of Activity
- Restrict and Limit Access

Technical Measures:

- Must use at least simple, low-cost defenses
- Complex and Unique Passwords
- Two-Factor Authentication
- Segment Network
- Endpoint Security (Antivirus)
- Secure Access
- Encryption
- Cybersecurity Software
- Monitoring Activity on Network
- Verify and Test Defense

Physical Measures:

- Put Security Measures in Writing
- Physical Files
- Protect Devices
- Keep Physical Devices Safe and Secure
- Dispose of Paperwork
- Dispose of Equipment
- Backup Data Access

What Does Reasonable Security Mean in California?

- 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 PRA based, in part, on a business’s failure to implement reasonable security.
- No CA law defines “reasonable security.”
- In 2016, the CA AG’s Office suggested that a company that complied with the 20 minimum security controls reflected in the Center for Internet Security‘s Critical Security Controls (“CIS Controls”) would meet this requirement.
- The AG’s Office also suggested the failure to establish and document compliance with the CIS Controls would constitute a lack of reasonable security.

CIS. Center for Internet Security®

Insight from Cases Examining Reasonable Security in California

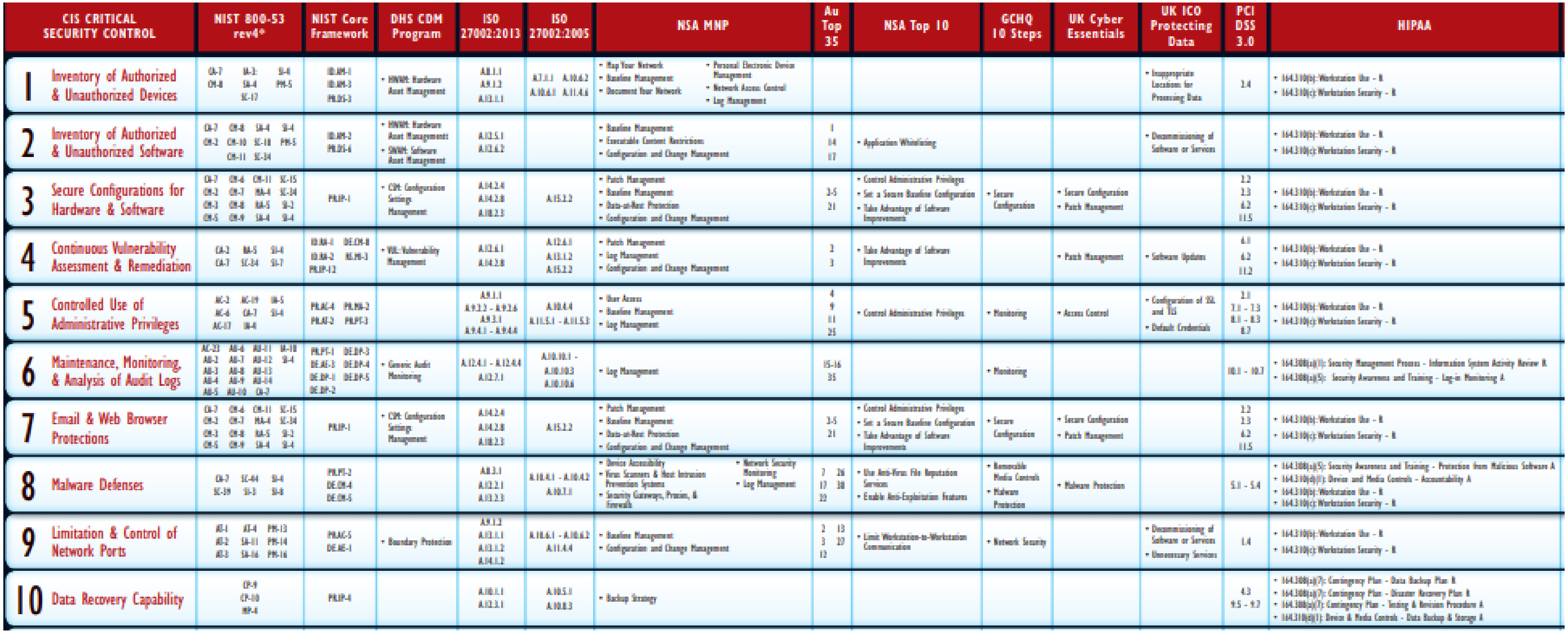
Plaintiffs have made it past the pleading stage where they alleged defendants failed to employ reasonable security by:

- Failing to adopt industry-standard encryption, including on point-of-service (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

Mapping Security Controls Across Regimes



CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA
1 Inventory of Authorized & Unauthorized Devices	CA-7 IA-3 SI-4 CM-8 SA-4 PM-5 SC-17	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Management • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 SI-4 AC-17 IA-4	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 - 10.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.13.2.3	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1): Device and Media Controls - Accountability A • 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
9 Limitation & Control of Network Ports	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.3 9.5 - 9.7	• 164.308(a)(7): Contingency Plan - Data Backup Plan R • 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7): Contingency Plan - Testing & Revision Procedure A • 164.310(d)(1): Device & Media Controls - Data Backup & Storage A

Utilize an industry-accepted standard like the CIS 20 Critical Security Controls as a starting point and then compare other regimes' controls.

A/C Privilege and Work Product Protection

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

Work Product Protection – Materials prepared in anticipation of litigation.

Try and ensure any investigation and related materials are protected

- Involve counsel immediately; incorporate counsel into your incident response plan.
- 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 counsel.
- 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.

CCPA Case Monitoring

- Given the 30-day cure, should not see CCPA PRA cases until February 2020
- **2019**
  - Cases already referenced CCPA
  - *Capital One and AWS case*: alleged CCPA violation for failure to implement adequate and reasonable data security measures to protect customer data
- **2020**
- *Hannah Anderson and Salesforce case:*
  - Data breach occurred Sept. through Nov. 2019. Customers and Attorneys General were notified of the breach on January 15, 2020.
  - Allegations that Defendants violated California's California Consumer Privacy Act by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.
  - Other cases mentioning CCPA

Unresolved Questions About CCPA Enforcement

Private Right of Action

1. What is reasonable security?

2. Will plaintiffs be able to expand the definition of personal information to the broad CCPA definition?

3. Can a defendant cure a breach? Pay the value of the data?

4. What is the statute of limitations?

5. Will the plaintiffs' bar be able to expand PRA to general compliance enforcement (UCL)?

Proactive Next Steps

1. Lay groundwork for your defenses

- ✓ Cure - take reasonable corrective action, act to ensure no future incidents, etc.
- ✓ Access + disclosure = acquisition
- ✓ Reasonable security - adopt industry-accepted standards, document efforts, etc.

2. Take steps now to mitigate effects

- ✓ Include arbitration provisions and class action waivers in agreements.
- ✓ Update insurance coverage - policies to cover regulatory fines and cost of civil litigation.
- ✓ Revise vendor agreements to include indemnification provisions where vendor breach.
- ✓ Carefully word breach notices to avoid giving plaintiffs' counsel roadmap.

3. Adopt incident response best practices

4. Focus on information security/reasonable security

- ✓ Map out regulatory requirements re information security; address gaps.
- ✓ Regularly update policies and procedures, particularly when business changes.
- ✓ Avoid successive breaches at all costs.

CCPA Enforcement

CCPA Enforcement Measures

- **Attorney General** – Empowered to seek penalties of $2,500-$7,500. Expansive enforcement powers. May take over consumer actions.
  - $2,500 for each violation; $7,500 for intentional violations
  - Civil penalties and settlement funds to be deposited into Consumer Privacy Fund to offset costs of enforcement
  - Injunctive relief permitted
  - 30-day cure period
  - Third parties can seek opinion of the AG for guidance on how to comply with its provisions
  - Non-compliance violations prior to July 1, 2020, fair game

When and Where Will We See AG Enforcement?

- **Timeline:**
  - CCPA Effective Jan. 1, 2020; AG Enforces July 1, 2020; AG Regulations not final
  - Several ad groups asked AG Becerra to delay CCPA enforcement in early January
  - CA AG Regulations Issued Comments on February 7, 2020
- **Issues:**
  - Varying interpretations of “Sale” under the CCPA
  - Interpretation of valuable consideration
  - Can affiliates be part of a single business?
  - Who will the CA AG target?
  - Will the AG delay enforcement?
  - Will the plaintiffs’ bar or local district attorneys be able to find a way to enforce the CCPA?

Overlapping Issues Between GDPR & CCPA

- GDPR continues to set baseline for global privacy and data protection discussions.
- Although very different, the GDPR experience may translate to CCPA, including:
  - (1) high costs of compliance for all companies
  - (2) last minute preparation or “wait and see” approach
  - (3) fewer data subject requests than expected, but targeted requests from activists
  - (4) enforcement includes smaller/mid-size companies (easier to build case against)
  - (5) particularly difficult application to the advertising ecosystem
  - (6) ramp up in enforcement as regulatory bodies increase staff and expertise.
- Some U.S. privacy activists have threatened to use contradictions in companies’ reporting under the GDPR and CCPA as basis for U.S. lawsuit (deceptive claims).
- Some U.S. privacy activists and lawmakers are pushing for the adoption of GDPR-like measures at the federal level (e.g., consent, strong enforcement, etc.).

Cyber Insurance in Light of CCPA

- Will enforcement fines be covered?
- Will litigation costs related to PRA be covered?
- How are insurers approaching the coming storm?

A Federal Fix?

What About a Federal Fix?

- Members of the Senate Committee on Commerce, Science and Transportation have introduced competing bills
- Activity across houses in Congress
- Empower federal agency?
- Private right of action
- Scope of preemption
- Address “sensitive” data

Senate Working Group

Akin Gump
STRAUSS HAUER & FELD LLP

Confidential – Not for Distribution Beyond Attendees

Federal Legislative Efforts

Senate Commerce Republicans

- **Preemption**: Yes
- **PRA**: No
- **Authority**: FTC existing authority
- **Data Security**: FTC certification programs to create standards
- **Rights**: access, correction, deletion, data portability

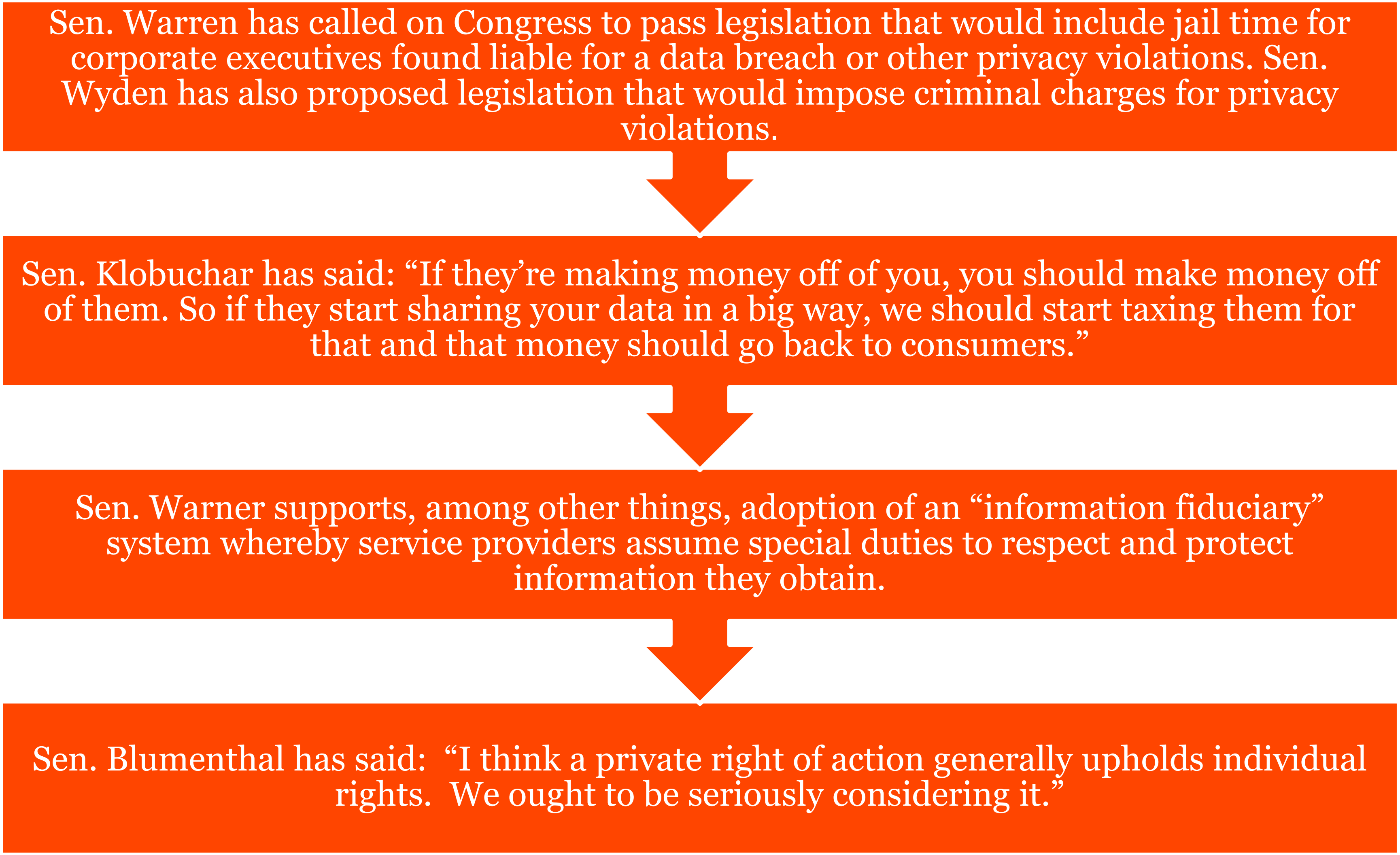
Senate Commerce Democrats

- **Preemption**: No
- **PRA**: Yes
- **Authority**: FTC new bureau and state AGs
- **Data Security**: Corporate privacy officers, FTC/NIST rulemaking
- **Rights**: access, correction, deletion, data portability

House Bipartisan Draft

- **Preemption**: No Language
- **PRA**: No Language
- **Authority**: FTC new privacy bureau
- **Data Security**: Annual assessments, FTC rulemaking, breach notification
- **Rights**: access, correction, deletion, data portability

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.

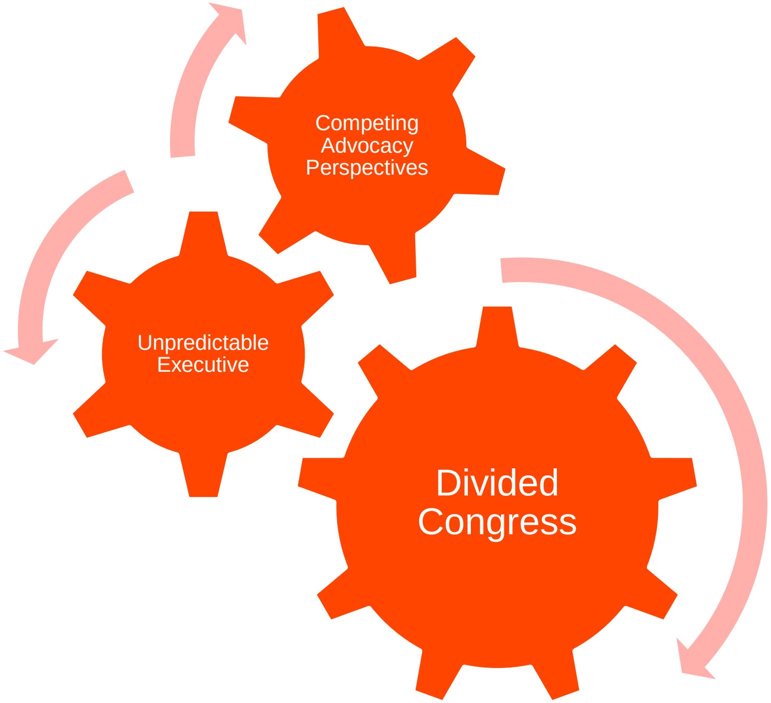
Sen. Klobuchar has said: “If they’re making money off of you, you should make money off of them. So if they start sharing your data in a big way, we should start taxing them for that and that money should go back to consumers.”

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. Blumenthal has said: “I think a private right of action generally upholds individual rights. We ought to be seriously considering it.”

Significant Uncertainty Remains

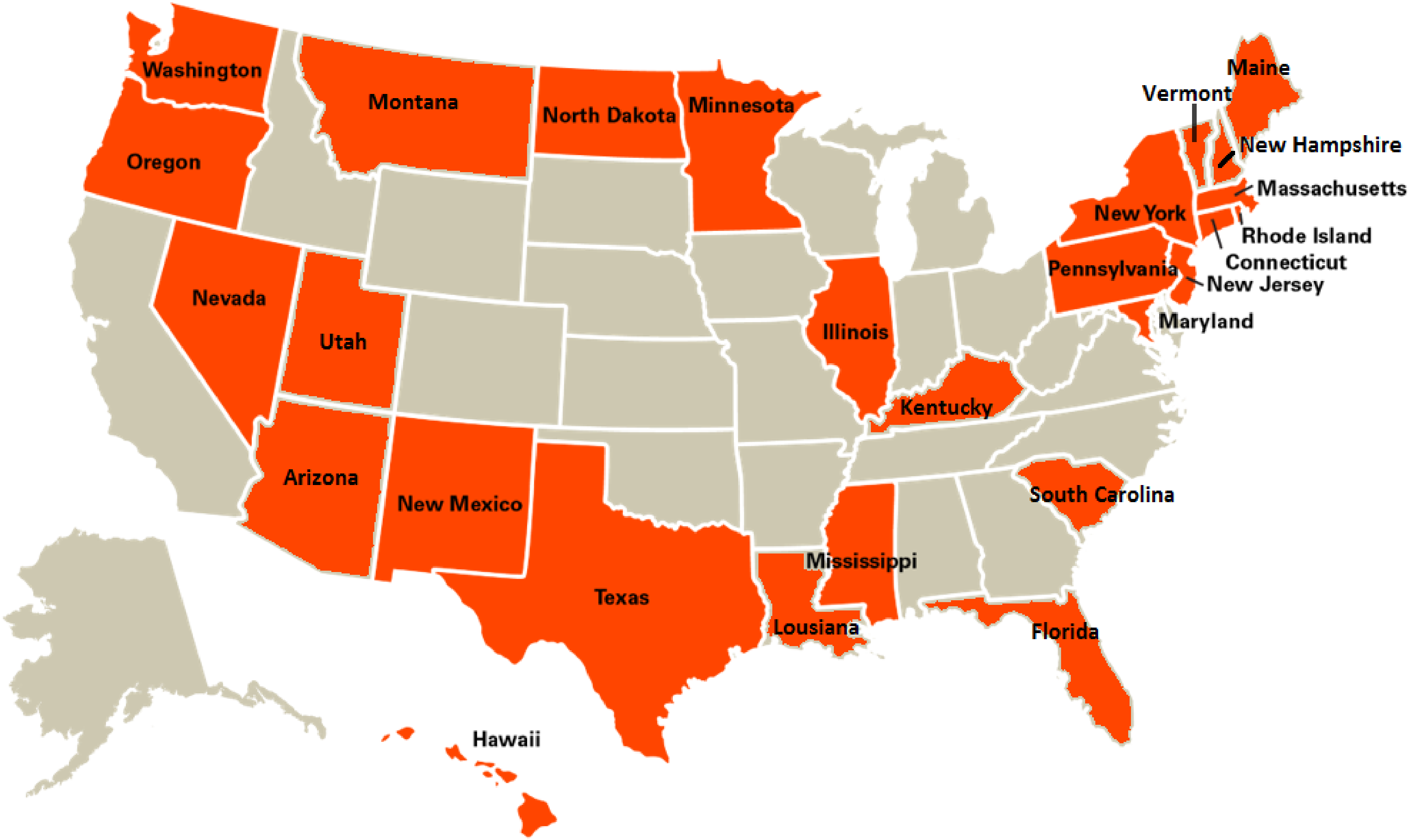
- Congressional approaches vary.
  - House vs. Senate.
  - Committee hearings.
  - Looming 2020 race.
- Motivated advocacy pushing agenda.
  - Industry advocates vs. consumer activists.
  - State regulators pushing their own role.
  - Federal preemption, PRA and rulemaking authority are key issues.
-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



Confidential – Not for Distribution Beyond Attendees

Other Similar Privacy Proposals

26 states have followed California, by introducing comprehensive privacy bills in 2019:



Confidential – Not for Distribution Beyond Attendees

Big Tech – Regulatory Enforcement Outlook

Regulatory Data Privacy Settlements of 2019

- **Facebook**
  - Fined a record-breaking $5 billion by FTC for data privacy violations related to Cambridge Analytica
  - Fined $100 million by SEC for its handling of Cambridge Analytica issues
- **Google/YouTube**
  - Fined $170 million by FTC for allegedly collecting personal data about children without parental consent, the largest monetary penalty the FTC has obtained in a COPPA case.
- **TikTok/Musical.ly**
  - Fined $5.7 million by FTC for allegedly collecting personal data about children without parental consent
- **Privacy Shield Enforcement**
  - FTC brought actions against a number of companies alleged to have made false claims of certification under the EU-U.S. Privacy Shield and continues to express that enforcement in this area is a high priority.

Confidential – Not for Distribution Beyond Attendees

Ongoing Investigations in 2020

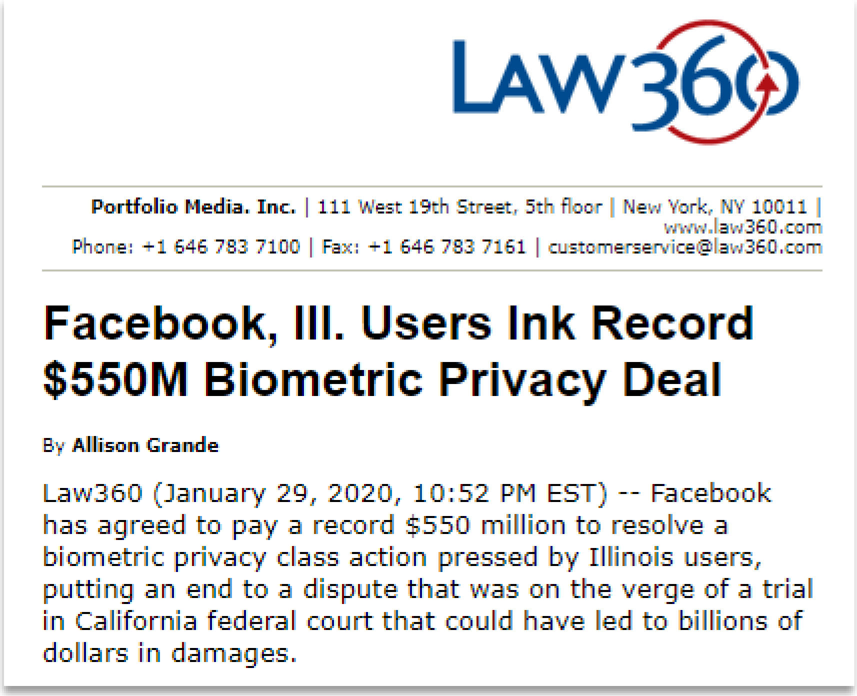
- **DOJ – Apple, Amazon, Google, Facebook, Others?**
  - Investigating whether “market-leading online platforms…are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers.” Attorney General Bill Barr has said DOJ will reach a determination this year.
- **FTC – Facebook and Amazon**
  - As part of its investigation, FTC has been reportedly considering an injunction against Facebook based on its data interoperability practices.
- **State AGs – Google and Facebook**
  - 47 state attorneys general have announced they are investigating Google and Facebook, at least in part due to “concerns over the control of personal data by large tech companies” and “anticompetitive practices that endanger privacy and consumer data.”
  - California AG is also separately investigating Facebook’s data privacy practices.

Efforts Toward (Self) Regulation

- **Facebook**
  - Facebook has committed to change the ways it uses personal data and enhance its oversight of third-party apps
  - Creation of an independent content oversight board
- **Google**
  - Privacy Sandbox Initiative including commitment to phase out third-party cookies on its Chrome browser by 2022
- **Microsoft**
  - Active engagement in Washington Privacy Law drafting, particularly regarding facial recognition technology provisions
  - “Strong federal privacy should not only empower consumers to control their data, it also should place accountability obligations on the companies that collect and use sensitive personal information.” – Julie Brill, Microsoft Corporate VP for Global Privacy and Regulatory Affairs and Chief Privacy Officer

Recent Biometric Privacy Developments

- Biometrics continue to be added to state data breach notification laws
- Continued trend of class action lawsuits stemming from Illinois' Biometric Information Privacy Act (BIPA)
- Increased scrutiny from regulators could lead to larger fines.
- Will we see a major biometric data breach in 2020?



LAW360

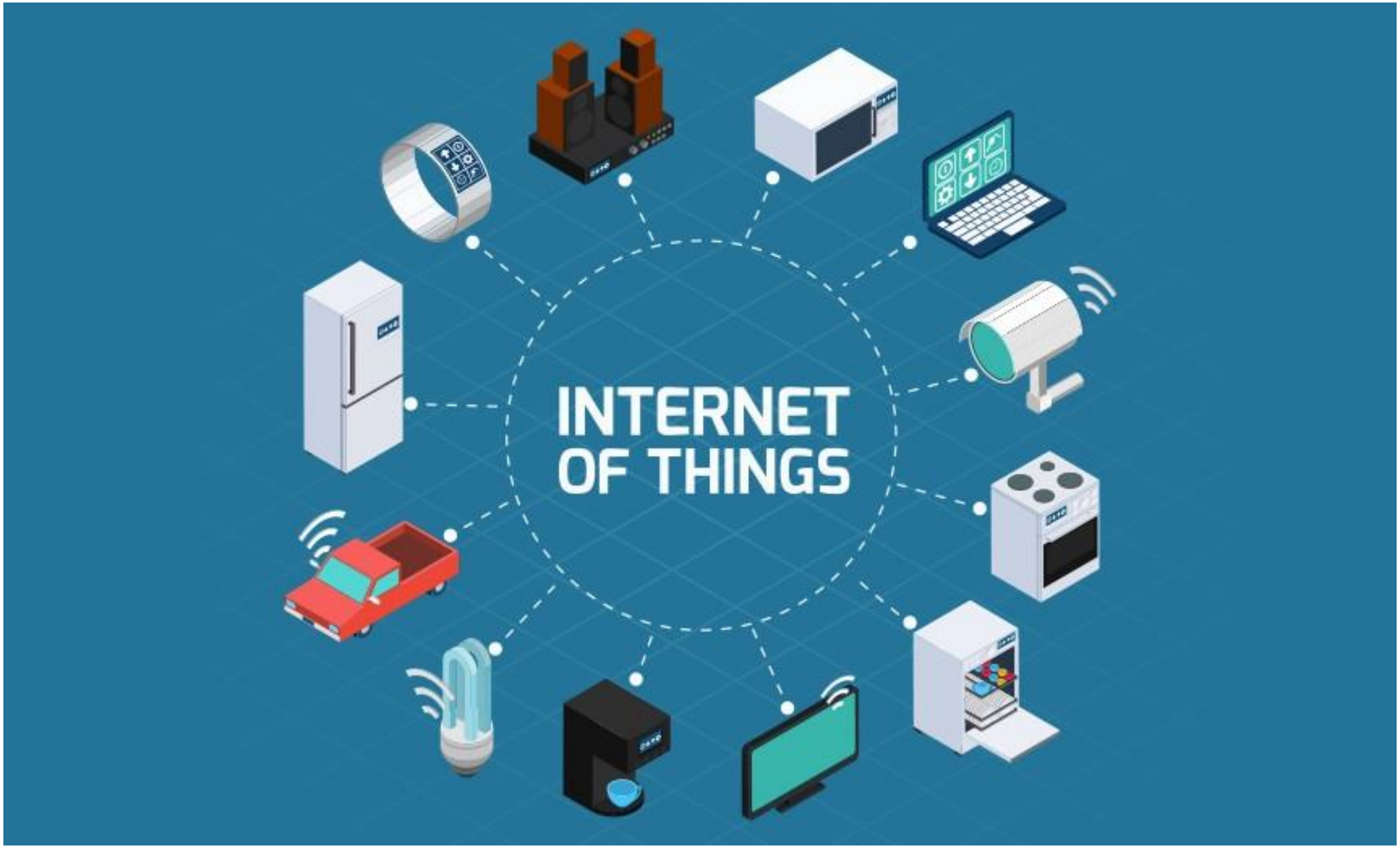
Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Facebook, Ill. Users Ink Record $550M Biometric Privacy Deal

By **Allison Grande**

Law360 (January 29, 2020, 10:52 PM EST) -- Facebook has agreed to pay a record $550 million to resolve a biometric privacy class action pressed by Illinois users, putting an end to a dispute that was on the verge of a trial in California federal court that could have led to billions of dollars in damages.

Developing Regulation of the Internet of Things



Confidential – Not for Distribution Beyond Attendees

The Coming Year+

Washington Privacy Act – Draft bill reintroduced in 2020

Children's Data and COPPA

ePrivacy/Cookies – Final text and developments with digital advertising.

CCPA 2.0 – New ballot initiative to strengthen CCPA and EU negotiations.

Harm & Value of Data – Push to put a price on data and utilize to establish harm.

Facial Recognition – Expensive litigation, expanding prohibitions, outcry.

Brexit impact on Privacy Shield and GDPR

Team Contact Information

Natasha Kohne, CIPP/US
Partner, Akin Gump Strauss Hauer & Feld LLP
San Francisco
T: +1 415.765.9505
nkohne@akingump.com

Michelle Reed, CIPP/US
Partner, Akin Gump Strauss Hauer & Feld LLP
Dallas
T: +1 949.885.4218
mreed@akingump.com

Amy Yeung, CIPP/US, CIPP/EU
General Counsel and Chief Privacy Officer, Lotame, Inc.
Washington, D.C.
T: +1 410.379.2195 x2005
ayeung@lotame.com

Anthony T. Pierce
Partner, Akin Gump Strauss Hauer & Feld LLP
Washington, D.C.
T: +1 202.887.4411
apierce@akingump.com