RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **LAW-M02**

Data Protection and Privacy Developments Around the World

MODERATOR: **Carla "CJ" Utter, JD, CISSP, CIPP EU/US**
VP-Legal, Privacy Counsel
Viant Technology

PANELISTS:

Ann Marie Mortimer, Esq.
Partner
Hunton & Williams LLP

Dominique Shelton Leipzig, Esq., CIPP/US
Partner, Cybersecurity & Data Privacy practice
Mayer Brown

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors or the individual's employers. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

MODERATOR:

Carla “CJ” Utter, JD, CISSP, CIPP EU/US

VP-Legal, Viant Technology

PANELISTS:

Ann Marie Mortimer, Esq.

Managing Partner
Hunton & Williams LLP

Dominique Shelton Leipzig, Esq. CIPP/US

Partner, Cybersecurity & Data
Privacy practice
Mayer Brown

Agenda

- CCPA-How Did We Get Here? Private Right of Action and Cyber Security Importance
- Cyber Security Data Breach and Privacy Litigation
- Recent CCPA Cases
- Privilege Under Scrutiny
- Recent Caselaw
- Other States: CPRA (CA), CO, VA, UT, CT
- SEC Cyber Security Proposed Reporting Rule
- Presidential Orders
- Other federal movements

CCPA-How Did We Get Here?

- The CCPA changed the entire privacy landscape in the U.S.
- Granted California “consumers” certain rights over their personal information
  - Right to access, delete and opt out of sale
- Requires businesses subject to the law to disclose specified, detailed content in the business’s privacy policies
- Provides certain benefits to businesses that contractually restrict the activities of service providers that process personal information
- Mandates specific CCPA training of relevant personnel
- Compliance deadline was January 1, 2020, enforcement July 1, 2020.
- Private right of action for data breaches

CCPA Private Right of Action

- CCPA gives consumers a private right of action when their "nonencrypted and nonredacted personal information" 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."
  - Unlike most data breach and privacy laws
  - No proof of actual harm
  - Statutory damages allowed

CCPA Cyber Security Requirements

- 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
  - CIS 20 (California's 2016 Data Breach Report)
  - NIST Cybersecurity Framework

Notable CCPA Cases

- Gardiner v. Walmart, 2021 WL 4992539 (N.D. Cal. July 28, 2021) (no CCPA retroactivity, failure to meet statutory requirements for PII)

- Hayden v. TRE, (C.D. Cal. May, 2022) (no CCPA retroactivity; private right of action limited to data breach),

Privilege Under Scrutiny

- Motivation of the investigation
- Was the report prepared in anticipation of litigation or would it have been done as part of normal business operations?
- Pre-existing relationship with investigator
- Courts have found against work-product privilege where Defendant had a pre-existing relationship with investigator.
- Hiring a new/separate investigator may weigh in favor of work-product privilege.
- Recipients of report
- Sharing report with non-legal personnel weighs against privilege.
- Sensitivity of business
- In determining whether an investigation was done for purely litigation purposes, courts have considered the sensitivity of the defendant's business. If security is a key business concern, Defendants may be likely to conduct investigation, regardless of litigation threat. This weighs against work-product privilege.
- Characterization of expenses
- Was investigation characterized as a legal or business (non-legal) expense?

Notable Cases – Disclosure Ordered

- In re Polaris, Inc., 967 N.W.2d 397, 410-11 (D. Minn. 2021) - "primary purpose" of investigation was not legal advice where report provided recommendations on corporate policy addressed regulatory concerns
- In re Rutter's Data Security Breach Litig., 2021 WL 3733137, at *3 (M.D. Pa. July 22, 2021) - corporate deponent stated litigation "was not contemplated" when investigation began and report was shared with non-legal personnel
- In Re Capital One Customer Data Security Breach Litigation, 2020 WL 2731238, at *4 (E.D. Va. May 26, 2020) – Defendant likely would have investigated security breach regardless of threat of litigation, investigator's SOW was executed before breach and litigation, investigation costs were originally characterized as business expenses, and report was shared with non-legal personnel
- Wengui v. Clark Hill, PLC, 338 F.R.D. 7, 12 (D.D.C. 2021) – Defendant likely would have investigated security breach regardless of threat of litigation and report was used for non-legal purposes and shared with non-legal team

Notable Cases – Disclosure Was Not Ordered

- In re Target Corp. Customer Data Security Breach Litig., 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015) - Defendant engaged a new investigator after breach, whose sole purpose was to advise the legal team

- In Re Experian Data Breach Litig., 2017 WL 4325583, at *3 (C.D. Cal. May 18, 2017) - report was only shared with in-house legal department and outside counsel

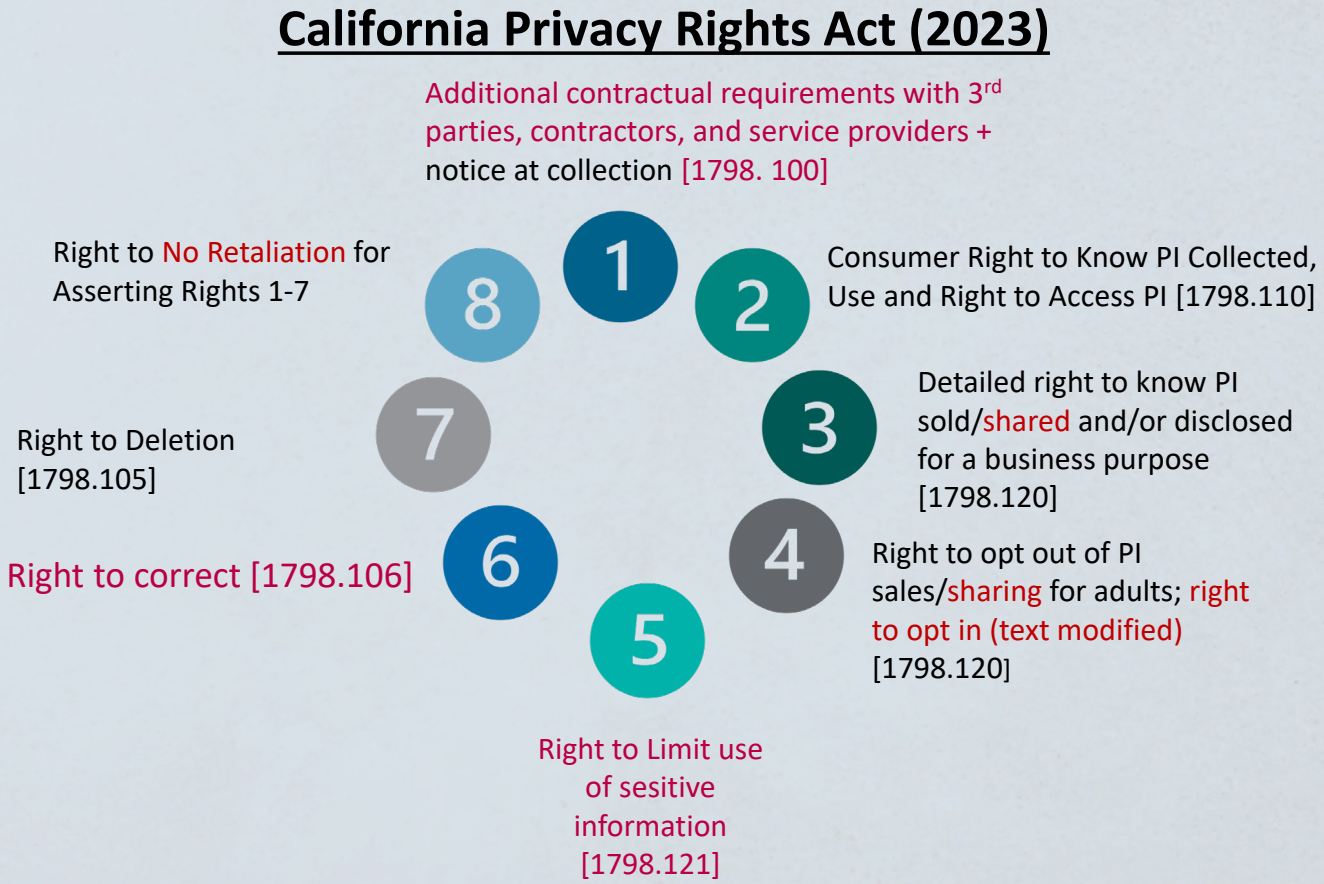
Other States Privacy Laws

- CPRA (CA again)
- Colorado
- Virginia
- Utah
- Connecticut

CPRA-California Privacy Rights Act

New Legal Developments: CPRA

- B2B and human resources data now within scope of legal regimes



CPA- Colorado Privacy Act

- July 1, 2023
- Difference: No revenue thresholds, applies to controllers and processors
- Does not exempt nonprofits
- The CPA exempts certain types of data subject to state and federal laws: HIPAA, FCRA, COPPA and others
- Personal data is defined under the CPA as “information that is linked or reasonably linkable to an identified or identifiable individual.”
  - Difference: It does not include employment data, de-identified or publicly available data
  - Regulates sensitive data
  - No Private Right of Action, CA AG and DA enforcement

CPA Consumer Rights and Consent

- (1) the right to opt out of any processing for purposes of targeted advertising, sale to third parties, or profiling in connection with decisions that produce legal or similarly significant effects;
- (2) the right to access, correct or delete their personal data;
- (3) the right to obtain a portable copy of their personal data
- Consent:
  - may not be given via: (a) “acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;” (b) “hovering over, muting, pausing, or closing a given piece of content;” or (c) “agreement obtained through dark patterns”

Business Obligations for CPA

- Similar to the CPRA and Virginia Privacy Law:
  - Duty of transparency and purpose specification
  - Duty of data minimization
  - Duty to avoid secondary use
  - Duty to avoid unlawful discrimination
  - Opt in for sensitive data processing
  - Duty of care: A controller must take “reasonable measures to secure personal data during both storage and use from unauthorized acquisition,” and those measures must “be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business”
  - Duty to conduct and document data protection assessment
    - CO AG can request these copies (enumerated in law)

VCDPA-Virginia Consumer Data Protection Act

- January 1, 2023
- Scope: VCDPA applies to all entities “who conduct business in the commonwealth of Virginia or produce products or services that are targeted to residents of the Commonwealth” and, during a calendar year, either:
- (1) control or process personal data of at least 100,000 Virginia residents, or
- (2) derive over 50% of gross revenue from the sale of personal data (though the statute is unclear as to whether the revenue threshold applies to Virginia residents only) and control or process personal data of at least 25,000 Virginia residents.

VCDPA-Virginia Consumer Data Protection Act

- "personal data" defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person," but excludes employment data, pseudonymous data and "de-identified data or publicly available information."
- Consumer rights mirror CPRA
- Grants consumers the right to opt-out of the sale of personal information for "monetary" (as opposed to "valuable") consideration by the controller to a third party

VCDPA-Virginia Consumer Data Protection Act

- Data processing agreements and data impact assessments required.
- No private right of action
- Companies must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data," as appropriate to the volume and nature of the personal data at issue (make sure your contracting parties are not watering this language down).
  - See also New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act

UCPA-Utah Consumer Privacy Act

- December 31, 2023
- Scope: for-profit entities ("controllers" or "processors") that (1) conduct business in Utah or target products and services to consumers who are residents of the state, (2) have annual revenues of at least $25 million, *and* (3) meet one of two threshold requirements:
  - Annually control or process the personal data of 100,000 or more Utah residents ("consumers"); *or*
  - Derive over 50 percent of gross revenue from the "sale" of personal data and control or process personal data of 25,000 or more consumers.
- Personal data definition mirrors CO and VA
- Exemptions for federally regulated entities (i.e. HIPAA, FCRA), tribes, etc.
- Same consumer rights as CO. No appeal of denial right

UCPA-Utah Consumer Privacy Act

- Required to have a written contract between the controller and processor
- Difference: must only provide notice and chance to opt out prior to processing consumer's sensitive data (or comply with the Children's Online Privacy Protection Act (COPPA) for the sensitive data of children under 13)
- Difference: Does not give consumers a right to opt out of profiling
- Difference: No requirement to conduct data protection assessments
- Enforcement: Utah Division of Consumer Protection may investigate consumer complaints under the UCPA and refer complaints to the attorney general. No private right of action

Connecticut Privacy Law

- July 1, 2023
- applies to persons that conduct business in Connecticut or produce products or services that are targeted to residents of the state, and that control or process the personal data of a particular number of residents, namely either:
  - 100,000 or more Connecticut residents, excluding residents whose personal data is controlled or processed solely for the purpose of completing a payment transaction; or
  - 25,000 or more Connecticut residents, where the business derives more than 25% of its gross revenue from the sale of personal data
- allows consumers to opt out of the processing of their personal data for purposes of (a) targeted advertising, (b) the sale of personal data, and (c) profiling in furtherance of solely automated decisions that produce similarly significant effects

Connecticut Privacy Law

- No private right of action, enforced by the AG
- Until December 31, 2024, enforcement actions will be subject to 60-day cure period; thereafter, the attorney general may, but is not required to, provide an opportunity to correct an alleged violation
- Could be up to $5000 per offense fine

SEC Cyber Security Proposed Reporting Rule

- SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule (March 9, 2022)
  - The SEC is proposing to amend Form 8-K to require current disclosure of material cybersecurity incidents. *Id.* at 12.
    - Notice within 4 days of the discovery of a material security incident. *Id.* at 20
  - The SEC is also proposing to add new Item 106 of Regulation S-K that would require a registrant to:
    - (1) provide updated disclosure in periodic reports about previously reported cybersecurity incidents;
    - (2) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning and capital allocation; and
    - (3) require disclosure about the
      - board's oversight of cybersecurity risk,
      - management's role in assessing and managing such risk,
      - management's cybersecurity expertise, and
      - management's role in implementing the registrant's cybersecurity policies, procedures, and strategies. *Id.* at 12.
  - The SEC is also proposing to amend Item 407 of Regulation S-K to require disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise. *Id.* at 12.

SEC Cyber Security Proposed Reporting Rule

- The SEC specifically noted the relationship between privacy and cybersecurity:

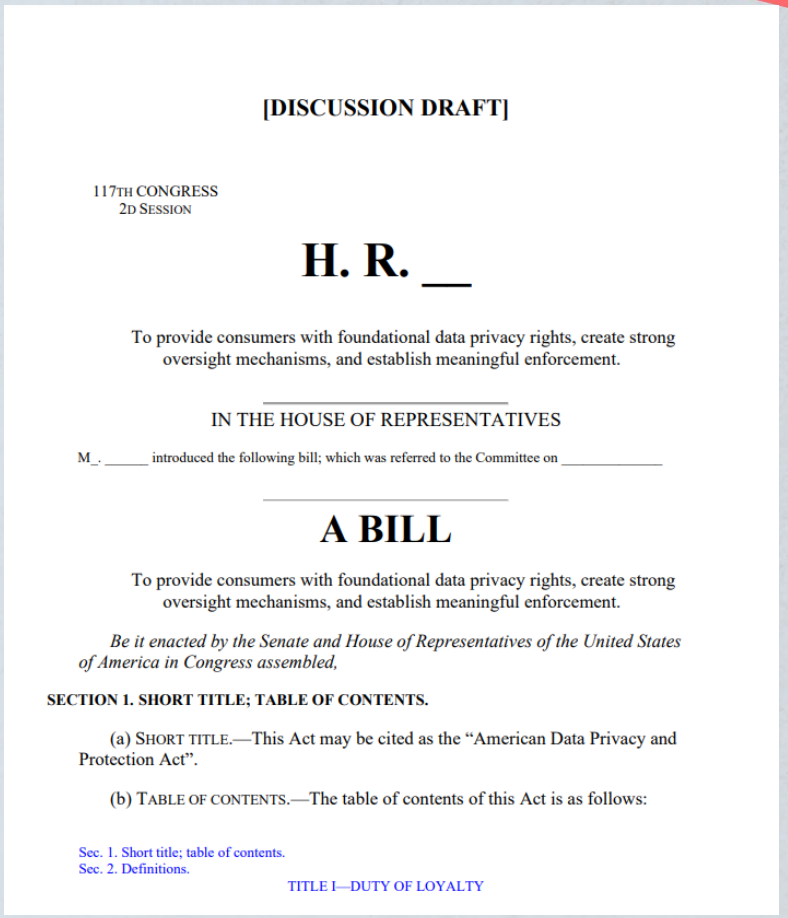
"The cost to companies and their investors of cybersecurity incidents is rising and doing so at an increasing rate. The types of costs and adverse consequences that companies may incur or experience as a result of a cybersecurity incident include the following:

. . .

- Harm to employees and customers, **violation of privacy laws**, and reputational damage that adversely affects customer or investor confidence." Id. 9- 10.

Federal Actions

- Federal Privacy Law
  - Social justice may be the driving force
- Agreement on
  - Preemption
  - Private Right of Action
  - Civil Rights/Anti-Discrimination
- Stumbling block
  - Mandatory arbitration clause, no class relief.



[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. __

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "American Data Privacy and Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
TITLE I—DUTY OF LOYALTY

Presidential Orders

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems,

BRIEFING ROOM

FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies

MAY 04, 2022 • STATEMENTS AND RELEASES

Today, President Biden will sign two Presidential directives that will advance national initiatives in quantum information science (QIS), signaling the Biden-Harris Administration's commitment to this critical and emerging technology. Together, the two directives lay the groundwork for continued American leadership in an enormously promising field of science and technology, while mitigating the risks that quantum computers pose to America's national and economic security.

The United States has long been a global leader in the development of new technologies, like QIS. QIS is a broad field of science and engineering. Quantum computers, one of the many promising applications of QIS, are not a replacement to traditional computers. Rather, they are a fundamentally different kind of computer, with the ability to analyze information in ways that traditional computers cannot. While QIS itself is not new, recent breakthroughs in QIS have shown the potential to drive innovations across the American economy, from energy to medicine, through advancements in computation, networking and sensing. Breakthroughs in QIS are poised to generate entirely new industries, good-paying jobs, and economic opportunities for all Americans.

President Biden will sign an Executive Order to foster these advances by furthering the President's commitment to promoting breakthroughs in cutting-edge science and technology. It does so by enhancing the National Quantum Initiative ↗ Advisory Committee, the Federal Government's principal independent expert advisory body for quantum information science and technology. The EO places the advisory committee directly under the authority of the White House, ensuring that the President, Congress, Federal

Action Items: Key Takeaways

- Have discussions with board and executives about upcoming privacy laws. Where do you do business? Risk vs. Benefit
- Determine your company's risk tolerance. Are you going to tune to the most restrictive and then cover the deltas from other laws?
- Think about privilege and what you put in writing
- Look at your cyber security stance and determine where there are control gaps and if you are certified to any standard.

Action Items: Key Takeaways

- Have discussions with board and executives about upcoming privacy laws. Where do you do business? Risk vs. Benefit
- Determine your company's risk tolerance. Are you going to tune to the most restrictive and then cover the deltas from other laws?
- Think about privilege and what you put in writing
- Look at your cyber security stance and determine where there are control gaps and if you are certified to any standard.