Lesson #1: There is tremendous value in having strong and clear indemnification clauses for data security incidents in vendor agreements.

Kronos Security Breach

- 12/11/21 – Ultimate Kronos Group discovered the Kronos Private Cloud was compromised by a ransomware attack

Kronos provides human resource management services such as payroll, attendance and scheduling for organizations

Customers used certain Kronos functions to track employee time entry, and to calculate and track pay including overtime or holiday pay. While offline time clocks still worked, Kronos and its customers were unable to access or collect that data.

Some data was exfiltrated

12/29/21 – Kronos announces plan for restoration by end of January

Kronos Saas Terms and Conditions

12.0 DATA SECURITY

12.1 As part of the Services, Kronos shall provide administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Customer data. Customer acknowledges that such safeguards endeavor to mitigate security incidents, but such incidents may not be mitigated entirely or rendered harmless. Customer should consider any particular Kronos supplied security-related safeguard as just one tool to be used as part of Customer's overall security strategy and not a guarantee of security. Both parties agree to comply with all applicable privacy or data protection statutes, rules, or regulations governing the respective activities of the parties under the Agreement.

Kronos Saas Terms and Conditions

13. INDEMNIFICATION

13.1 Kronos shall defend Customer and its respective directors, officers, and employees (collectively, the "**Customer Indemnified Parties**"), from and against any and all notices, charges, claims, proceedings, actions, causes of action and suits, brought by a third party (each a "**Claim**") alleging that the permitted uses of the Services infringe or misappropriate any United States or Canadian copyright or patent and will indemnify and hold harmless the Customer Indemnified Parties against any liabilities, obligations, costs or expenses (including without limitation reasonable attorneys' fees) actually awarded to a third party as a result of such Claim by a court of applicable jurisdiction or as a result of Kronos' settlement of such a Claim. In the event that a final injunction is obtained against Customer's use of the Services by reason of infringement or misappropriation of such copyright or patent, or if in Kronos' opinion, the Services are likely to become the subject of a successful claim of such infringement or misappropriation, Kronos, at Kronos' option and expense, will use commercially reasonable efforts to (a) procure for Customer the right to continue using the Services as provided in the Agreement, (b) replace or modify the Services so that the Services become non-infringing but remain substantively similar to the affected Services, and if neither (a) or (b) is commercially feasible, to (c) terminate the Agreement and the rights granted hereunder after provision of a refund to Customer of the Monthly Service Fees paid by Customer for the infringing elements of the Services covering the period of their unavailability.

Putting It Into Practice

- Educate contracts teams on importance of indemnification clauses
- Always negotiate into software contracts indemnification for data breaches or other cybersecurity events.
  - Alternatively, a Data Processing Agreement can be executed.

Lesson #2: “Selling” data doesn’t require a sale.

California Consumer Privacy Act

- The CCPA gives consumers the right to direct a business not to sell their personal information to a third-party.
- “Sell” is expansively defined in the CCPA as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”
- The inclusion of the phrase "other valuable consideration" indicates that many different types of non-cash transactions may classify as a “sale” if the business receives any type of benefit in return for providing access to the personal information.

California Attorney General

- The California AG has taken the position that the disclosure of data is a "sale" under the CCPA when the vendor provides analytics or builds profiles using the data
- The California AG's enforcement cases also indicate a focus on the use of data.

AG Enforcement

AG Enforcement Example: Cookies

- **Industry**: Consumer Electronics
- **Issue**: Sales of Personal Information
- A business that sells electronics maintained third-party online trackers on its retail website that shared data with advertisers about consumers' online shopping. The business neither imposed a service provider contractual relationship on these third parties, nor processed consumers' requests to opt-out that were submitted via a user-enabled global privacy control, e.g., a browser extension that signaled the GPC.
- After being notified of alleged noncompliance, the company worked with its privacy vendor to effectuate consumer opt-out requests and avoid sharing personal information with third parties under conditions that amounted to a sale in violation of the CCPA.

What Does This Information Tell Us?

- The California AG's enforcement activity indicates that it is focusing on *how* data is being used (and not on whether money was exchanged in consideration for the data).

Putting it into Practice

- Understand how all vendors use your data.
  - Pay particular attention to vendors who provide marketing and analytics services.
- Run cookie scans periodically across all your domains to understand the cookies and tags that your website is using.
- If you have already implemented a “Do Not Sale My Personal Information,” then ensure those cookies have been appropriately categorized.

What is “selling” under the California Consumer Privacy Act?

In general, any transfer or disclosure of personal information about a California consumer to a third party in exchange for consideration, regardless of whether money is exchanged, would qualify as a “sale” under CCPA

Does your entity “sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate” Personal Information about a California resident to another entity for “monetary or other valuable consideration”?

Valuable consideration is a broad term that may include development, enhancement, modification, or improvement of technologies, tools, methodologies, services, and offerings, or for development or performance of data analysis or other insight-generation beyond the contracted business service.

If NO, No Sale

If YES: Do you disclose that Personal Information SOLELY:

- At a consumer’s direction?
- To alert third party that consumer has submitted an opt-out request?
- As part of a merger, acquisition, bankruptcy, or other transaction which third party assumes control of all or part of the business?
- To comply with a legal obligation?
- To a Service Provider subject to:
  - Contractual restrictions that prohibit “retaining, using, or disclosing” Personal Information for any purpose other than “for the specific purpose of performing the services specified in the contract;
  - A certification made by Service Provider that it understands its contractual restrictions; and
  - Your company providing sufficient notice to consumers?

If NO, Sale

If YES, No Sale

Lesson #3: Don’t assume state privacy laws will follow California – or each other.

New Privacy Laws

- **California Privacy Rights Act (CPRA) (11/3/20)**
  - Effective January 1, 2023
- **Virginia Consumer Data Protection Act (VCDPA) (3/2/21)**
  - Effective January 1, 2023
- **Colorado Privacy Act (CPA) (7/7/21)**
  - Effective July 1, 2023

Just a Few Key Differences

- CPA and VCDPA only protect information about consumers acting as individuals, not as employees; CPRA applies to information about consumers *and* employees.
- CPA and VCDPA provide individuals the right to appeal a business' response to an access or deletion request; CPRA does not provide such a right.
- CPRA definition of "personal information" includes information that is linked to a household; CPA and VCDPA use a more narrow definition.

Contents of the Privacy Policy

Items Required	CCPA	CPRA	VCDPA	CPA
Categories of Data Collected/ Processed	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Sources from Which Data is Collected	✓ Yes	✓ Yes	✗ No	✗ No
Purpose of Collection/ Processing Data	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Categories of Data Shared	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Categories of Third Parties with Which Data is Shared	✓ Yes	✓ Yes	✓ Yes	✗ No
Description of Consumer Rights	✓ Yes	✓ Yes	✗ No	✓ Yes
Means to Exercise Consumer Rights	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Disclosure of “Selling” Practices and Method to Opt-Out	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Disclosure of Targeted Advertising Practices and Method to Opt-Out	✗ No	✓ Yes	✓ Yes	✓ Yes
Description of the Process Used to Verify Consumer Requests	✓ Yes	✓ Yes	✗ No	✗ No
Authorized Agent Instructions	✓ Yes	✓ Yes	✗ No	✗ No
Consumer Request Metrics	✓ Yes	✓ Yes	✗ No	✗ No
Date Last Updated	✓ Yes	✓ Yes	✗ No	✗ No

Vendor Contract Requirements

Explicit Prohibition on Sharing PI	✗ No	✓ Yes	✗ No	✗ No
Prohibition on Processing Outside the Specified Business Purpose	✓ Yes	✓ Yes	✗ No	✗ No
Prohibition on Combining PI with PI from Other Sources Outside the Business Purpose	✗ No	✓ Yes	✗ No	✗ No
Instructions for Processing	✗ No	✗ No	✓ Yes	✓ Yes
Nature and Purpose of Processing	✗ No	✗ No	✓ Yes	✗ No
Type of Data Subject Related to the Processing	✗ No	✗ No	✓ Yes	✗ No
Type of Personal Information Subject to the Processing	✗ No	✗ No	✗ No	✓ Yes
Processing Duration	✗ No	✗ No	✓ Yes	✓ Yes
Rights and Obligations of Both Parties	✗ No	✗ No	✓ Yes	✓ Yes
Notice and Opportunity to Object to Subcontractors	✗ No	✗ No	✗ No	✓ Yes
Duty of Confidentiality	✗ No	✗ No	✓ Yes	✓ Yes
Require Implementation of Technical and Organizational Security Measures	✗ No	✗ No	✗ No	✓ Yes
Return of Confidential Information	✗ No	✗ No	✓ Yes	✓ Yes
Provide Information Demonstrating Compliance	✗ No	✓ Yes	✓ Yes	✓ Yes
Reasonable Audits	✗ No	✓ Yes	✓ Yes	✓ Yes

Putting it into Practice

The Time Is NOW!

CPRA: January 1, 2023

Virginia: January 1, 2023

Colorado: July 1, 2023

Scope

Data Mapping/Inventory

Vendor Management

Operationalizing Consumer Rights

Revise External Documents

Lesson #4: Don’t assume reports generated in connection with a data security incident are privileged.

Why Does Privilege Even Matter

During IR, companies usually discover information that is both: (1) necessary to remediate and respond to the incident and (2) harmful to the company's defense should a regulatory investigation or lawsuit ensue.

Following a security incident, disputes frequently arise over whether IR documents (*e.g.*, forensic reports, analyses, and internal communications) are privileged or must be turned over.

Recent cases highlight that establishing protections involve a highly fact-sensitive inquiry and ultimately do not always weigh in the company's favor.

The law remains unsettled on when the attorney-client privilege and work product doctrine apply in the context of an incident investigation and the decision that a breach occurred and notice is required.

What Protections May Apply?

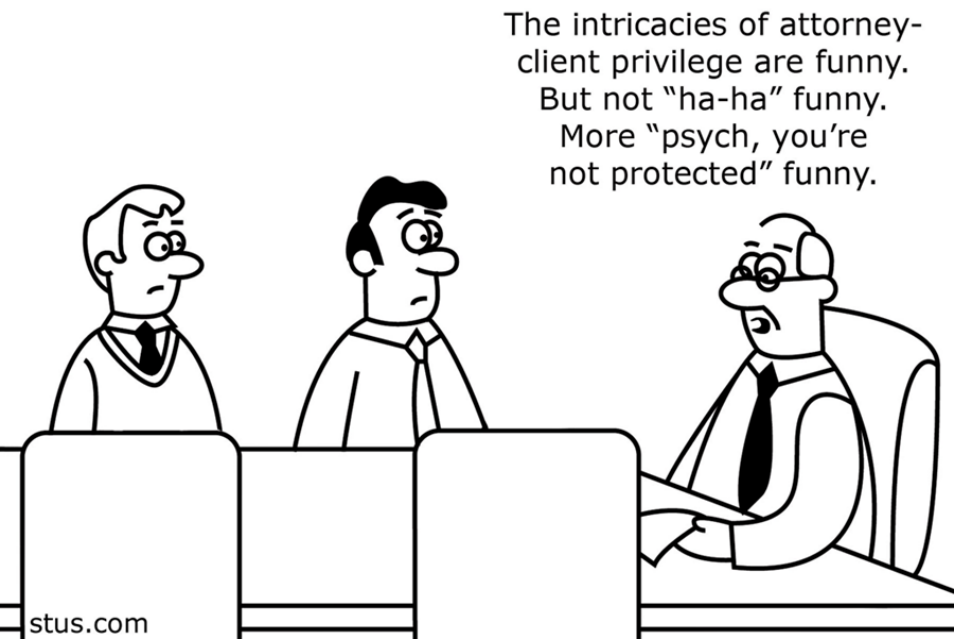
Attorney Client Privilege

- Protects confidential communications between lawyers and their clients that relate to the **request for, or rendering of, legal advice.**

Work Product Doctrine

- Protect documents or analyses performed by, or at the direction of, legal counsel **in anticipation of litigation.**
- Includes documents that would not have been created in substantially similar form but for the prospect of that litigation.

Privilege Isn't A Given



- The mere fact that communication is made to an attorney does not mean the communication is privileged.
- Materials are not automatically protected by the privilege merely because they are provided to or prepared by an attorney.
- Regulators may also have differing views on when privilege applies (e.g., NY DFS/CFPB).

Business Issue vs. Legal Issue (Focus is on the Why)

Action	Business	Legal
Determine root cause	Fix affected systems	Defend potential claims
Identify impacted data	Fix altered data for product functionality	Decide if notice is required
Containment	Prevent further damages to other systems	Determine contractual requirements (e.g. PCI)
Remediation	Improve security	Resolution options
Post Event Analysis	Fix administrative controls	Determine compliance with applicable standards

Putting it into Practice: Clark Hill and Capital One

1. Allow outside counsel to retain the forensic firm
2. Pay for litigation-related cybersecurity services from your litigation or legal budget.
3. Clearly define the legal advice sought and purpose in retainer agreement
4. Use the forensic report and related documents only for litigation purposes
5. Limit disclosure to necessary individuals.

Lesson #5: Cyber resilience must be a strategic focus in 2022.

Cyber Attacks Hit An All-time High

The most common cyberattacks are malware -- specifically ransomware -- and phishing.

- 48% of organizations found information-stealing malware activity in their technology in 2021. (Cisco)
- Approximately 37% of global organizations said they fell victim to some sort of ransomware attack in 2021. (IDC) – up 62% since 2019
- 86% of organizations had at least one user try to connect to a phishing site in 2021. (Cisco)

Increased remote work = increased risk

- Employees are biggest vulnerability
- 47% cited “distraction” as reason for clicking on a phishing email (real or test)

A Tale of Two Companies

Kronos

- Unclear
- Complete outage (since 12/11)
- Maybe restoration by end of January
- Multiple class action suits against customers
- Manual records, delayed tax information

JBS Food

- Shut down plants Australia, Canada and US
- Total downtime – 3 days
- No impact on food supply
- No class actions

Business Continuity

- Level of business continuity planning is the differentiator
- A company's ability to continue essential functions during an attack—and quickly resume full operations afterward—is critical to minimizing the direct and indirect costs of the attack.
- The length of downtime a company suffers is a critical factor in how destructive the attack will be to a company's revenue, resources, and reputation.

Putting It Into Practice

WISP

- Your Security Program Sets The Foundation For Business Continuity During An Outage
- There Is No Business Continuity Without An It Security Program
- Employee Training/Testing

Incident Response

- Business continuity and incident response are not the same.
- Containment
- Communication

Lesson #6: An ounce of CCPA prevention is worth a pound of cure.

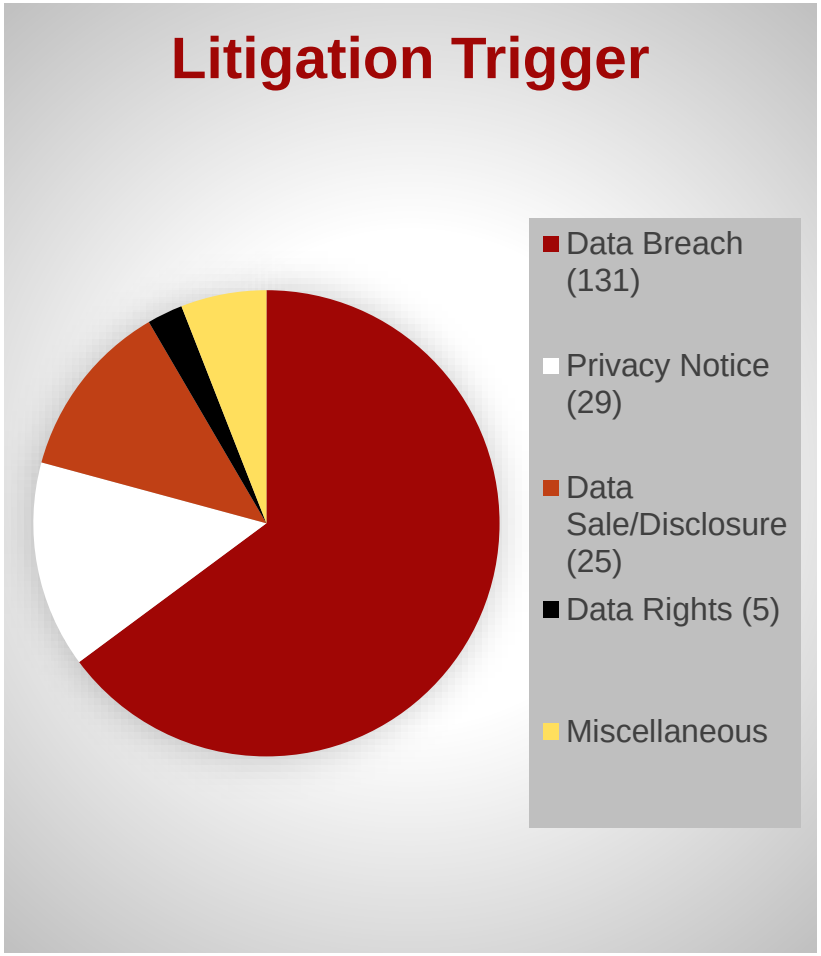
California Consumer Privacy Act

- **Private Right of Action**: CCPA allows consumers to bring an action for statutory damages in the event of a breach due to **failure to implement reasonable security procedures and practices**.

- **Pre-CCPA**: Difficulty in proving actual damages = low class action settlement payouts.

- **CCPA**: Actual damages or statutory damages between $100 and $750, whichever is greater.

Cases Filed



150+ CCPA-related actions filed

Case Theories:

- Data Breach
- Consumer Privacy Rights
- CCPA References (derivative claims)

Early Plaintiff Creativity

Ignoring the definitions of “personal information” in the California Consumer Records Act

Seeking to apply the CCPA beyond its geographic limits

Ignoring the limited scope of the private right of action

Seeking to use the CCPA as the standard of care for derivative claims - Unfair Competition Law (“unlawful” prong) and invasion of privacy (“protected interest,” “egregious breach,” and “community norms”)

Asserting claims for “unauthorized disclosure” based on voluntary data sharing by a business

Putting It Into Practice

- Review Your Privacy Policy
- Eliminate Unnecessary Promises
- Make A Strong Case for Reasonable Security

ACC Association of Corporate Counsel
SOUTHERN CALIFORNIA

20th ANNUAL IN HOUSE COUNSEL CONFERENCE

January 19, 2022

www.acc.com/chapters-networks/chapters/southern-california

#IHCC22