Top 5 Priorities for Getting Your Privacy House In Order In 2022

Association of Corporate Counsel All-Day MCLE La-LAW-palooza

Tuesday, April 26, 2022 | 9:30 a.m.

ACC Association of Corporate Counsel SheppardMullin

Your Presenters

Elizabeth Balfour
Litigation Partner
Sheppard Mullin

Wynter Deagle
Privacy Partner
Sheppard Mullin

Iris Sockel Mitrakos
Associate General Counsel
Mitchell International, Inc.,
(an Enlyte company)

Top 5 Priorities

Priority 1: Data Mapping and Retention

Priority 2: Vendor Contracts

Priority 3: Preservation Obligations v. Consumer Rights

Priority 4: Privilege in Incident Response

Priority 5: External Representations

DATA MAPPING AND RETENTION

Data Mapping

- You can’t manage what you don’t know you have.
- Accuracy is key.
- Map data, hardware and software so you know where your data lives. If we know better, we do better.
- Data mapping is also helpful in complying with CCPA/CPRA/GDPR obligations.
- Important to: draft disclosures, secure data, inform data retention policies and respond to requests beginning January 1, 2023

Other Value to a Data Map/Inventory

It shows us what data we have, including dark data that may not have been widely known to exist.

It allows us to identify which sources of data are trustworthy.

It allows us to see where we have data that is sensitive or subject to regulatory or policy controls.

It allows us to identify data that has value that is not being utilized/monetized.

It allows us to identify data that is risky and the benefits of maintaining it are not commensurate with that risk.

It allows us to see data that is subject to other controls such as a legal hold or investigations.

It helps inform roles and responsibilities so the organization can make intelligent business decisions about how to maximize the value of the data, minimize risks without interfering with investigations and legal processes or violating any regulation or policies.

What Is A Record?

- Records are the evidence of what an organization does.

- Records capture the business activities and transactions, correspondence, customer/client files, employee files, financial records.

- Where can records be found?

  - Electronic file management systems, the cloud, and physical storage spaces.

  - Examples: Emails, letters, memoranda, photographs, videos, text messages, instant messages (Slack, Zoom, Teams).

Record Retention Policy: Ensuring Compliance with Legal Requirements to Retain Records

- What is a Record Retention Policy?
- Best practice is to retain documents based on:
  - A contractual, statutory, or regulatory requirement.
  - Business need.
  - To preserve the ability to pursue or defend against a claim (litigation hold).
- Records are information assets and have value, when properly catalogued and organized.
  - Business units have a duty to stakeholders to manage records effectively, driving workforce efficiency.
  - Some records contain protected, proprietary or sensitive information that must be appropriately identified and safeguarded.

Record Retention Policy: Permission to Destroy

- California Privacy Rights Act goes into effect January 1, 2023.
- Document retention is front and center in the CPRA.
- At or before the point of collection, the business must inform consumers of "the length of time the business intends to retain each category of personal information … or if that is not possible, the criteria used to determine such period." Civil Code Section 1789.100(a)(3).
- The CPRA further requires that the retention of personal information "shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." Civil Code Section 1789.100(c).

Case Study: *In re InfoTrax (2019)*

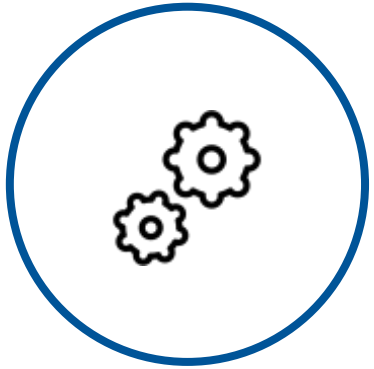
- FTC cited a business's ineffective record retention practices as a basis for a data security enforcement action.
- FTC listed the business's failure "to have a systematic process for inventorying and deleting consumers' personal information stored on InfoTrax's network that is no longer necessary," as one of the unreasonable security practices that led to multiple and repeated security breaches.
- As part of negotiated settlement, FTC required InfoTrax, among other things, to implement a comprehensive information security program that is subject to third-party biennial assessments *for the next 20 years*.

The Lifecycle Of A Record

Signs Of An Effective Record Retention program

Collaborative

Clear and Complete



Controlled

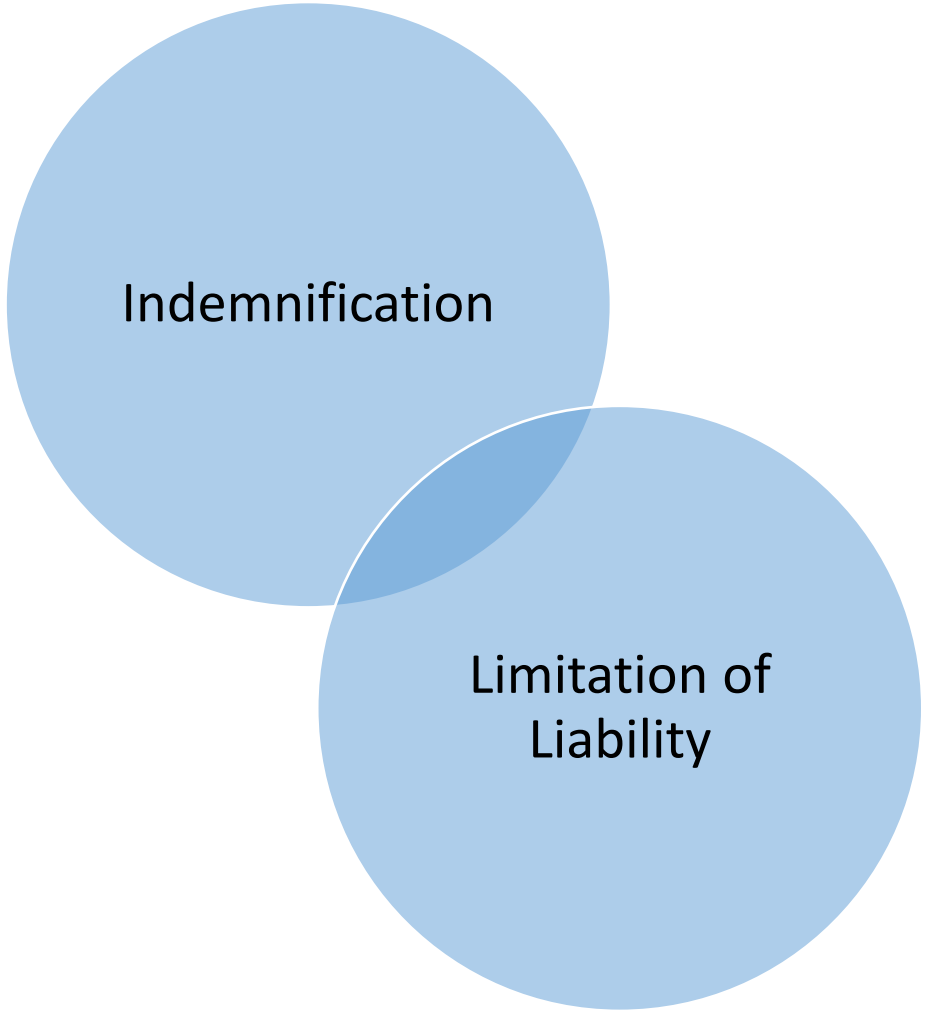
Compliant

VENDOR CONTRACTS

Contract Requirements

Items Required	CCPA	CPRA	VCDPA	CPA
Prohibition on Sharing PII	✗ No	✓ Yes	✗ No	✗ No
Prohibition on Processing Outside the Specified Business Purpose	✓ Yes	✓ Yes	✗ No	✗ No
Prohibition on Combining PII 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

HOTLY CONTESTED DPA TERMS



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 Fallout

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

THERESA MILERSON, individually and on behalf of all others similarly situated,

Plaintiff,

against

METROPOLITAN TRANSPORTATION AUTHORITY, NEW YORK CITY TRANSIT AUTHORITY, MANHATTAN AND BRONX SURFACE TRANSIT OPERATING AUTHORITY,

Defendants.

----------X

Case No.:

COLLECTIVE ACTION COMPLAINT

JURY TRIAL DEMANDED

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

JAMES CLICK, individually and on behalf of all others similarly situated,

v.

MERCEDES-BENZ USA, LLC, a Foreign Limited Liability Company

Case No. _____

FLSA Collective Action

PLAINTIFF'S ORIGINAL COLLECTIVE ACTION COMPLAINT

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA
PITTSBURGH DIVISION

DEVIN DROBSCH, individually and on behalf of all others similarly situated,

v.

PEPSICO, INC.

Case No. _____

FED. R. CIV. P. 23 Class Action

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA
HARRISBURG DIVISION

CORBIN HOLBERT and BRET GLIDEWELL, each individually and on behalf of all others similarly situated,

v.

THE GIANT COMPANY LLC

Case No. _____

CLASS/COLLECTIVE ACTION PURSUANT TO 29 U.S.C. §216(b) and FED. R. CIV. P. 23

PLAINTIFFS' ORIGINAL CLASS AND COLLECTIVE ACTION COMPLAINT

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.

Kronos SAAS Terms and Conditions

14. LIMITATION OF LIABILITY

14.1 EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMENT, KRONOS AND ITS SUPPLIERS WILL NOT BE LIABLE FOR ANY DAMAGES OR INJURIES CAUSED BY THE USE OF THE SERVICES OR BY ANY ERRORS, DELAYS, INTERRUPTIONS IN TRANSMISSION, OR FAILURES OF THE SERVICES.

14.2 EXCEPT FOR KRONOS' INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 13 ABOVE, THE TOTAL AGGREGATE LIABILITY OF KRONOS OR KRONOS' SUPPLIERS TO CUSTOMER AND/OR ANY THIRD PARTY IN CONNECTION WITH THE AGREEMENT SHALL BE LIMITED TO DIRECT DAMAGES PROVEN BY CUSTOMER, SUCH DIRECT DAMAGES NOT TO EXCEED AN AMOUNT EQUAL TO THE TOTAL NET PAYMENTS RECEIVED BY KRONOS FOR THE SERVICES IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE IN WHICH SUCH CLAIM ARISES.

14.3 EXCEPT FOR KRONOS' INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 13 ABOVE, IN NO EVENT SHALL KRONOS OR KRONOS' SUPPLIERS, THEIR RESPECTIVE AFFILIATES, SERVICE PROVIDERS, OR AGENTS BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY INCIDENTAL, SPECIAL, PUNITIVE, CONSEQUENTIAL OR OTHER INDIRECT DAMAGES OR FOR ANY LOST OR IMPUTED PROFITS OR REVENUES, LOST DATA OR COST OF PROCUREMENT OF SUBSTITUTE SERVICES RESULTING FROM DELAYS, NONDELIVERIES, MISDELIVERIES OR SERVICES INTERRUPTION, HOWEVER CAUSED, ARISING FROM OR RELATED TO THE SERVICES OR THE AGREEMENT, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH LIABILITY IS ASSERTED, WHETHER BREACH OF WARRANTY, INDEMNIFICATION, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, AND WHETHER LIABILITY IS ASSERTED IN CONTRACT, TORT OR OTHERWISE, AND REGARDLESS OF WHETHER KRONOS OR SUPPLIER HAS BEEN ADVISED OF THE

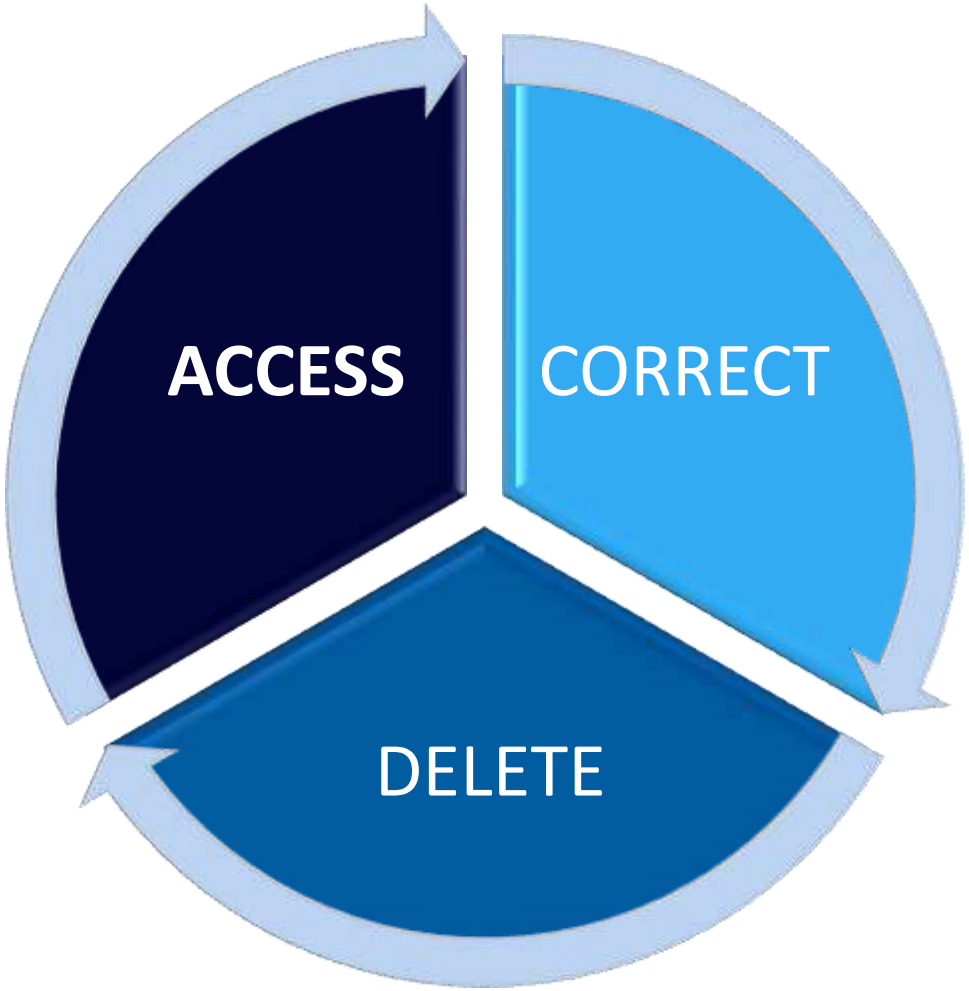
POSSIBILITY OF ANY SUCH LIABILITY, LOSS OR DAMAGE.

14.4 EXCEPT WITH RESPECT TO LIABILITY ARISING FROM KRONOS' GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, KRONOS DISCLAIMS ANY AND ALL LIABILITY, INCLUDING WITHOUT LIMITATION LIABILITY RELATED TO A BREACH OF DATA SECURITY AND CONFIDENTIALITY OBLIGATIONS, RESULTING FROM ANY EXTERNALLY INTRODUCED HARMFUL PROGRAM (INCLUDING WITHOUT LIMITATION VIRUSES, TROJAN HORSES, AND WORMS), CUSTOMER'S CONTENT OR APPLICATIONS, THIRD PARTY UNAUTHORIZED ACCESS OF EQUIPMENT, SAAS APPLICATIONS OR SYSTEMS, OR MACHINE ERROR.

Putting It Into Practice

DOCUMENT PRESERVATION V. CONSUMER RIGHTS

Consumer Data Rights



PRESERVING PRIVILEGE IN DATA SECURITY INCIDENT RESPONSE

Why Does Privilege Matter During IR?

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

- "Reasonable security measures" / Negligence

What Protections May Apply?

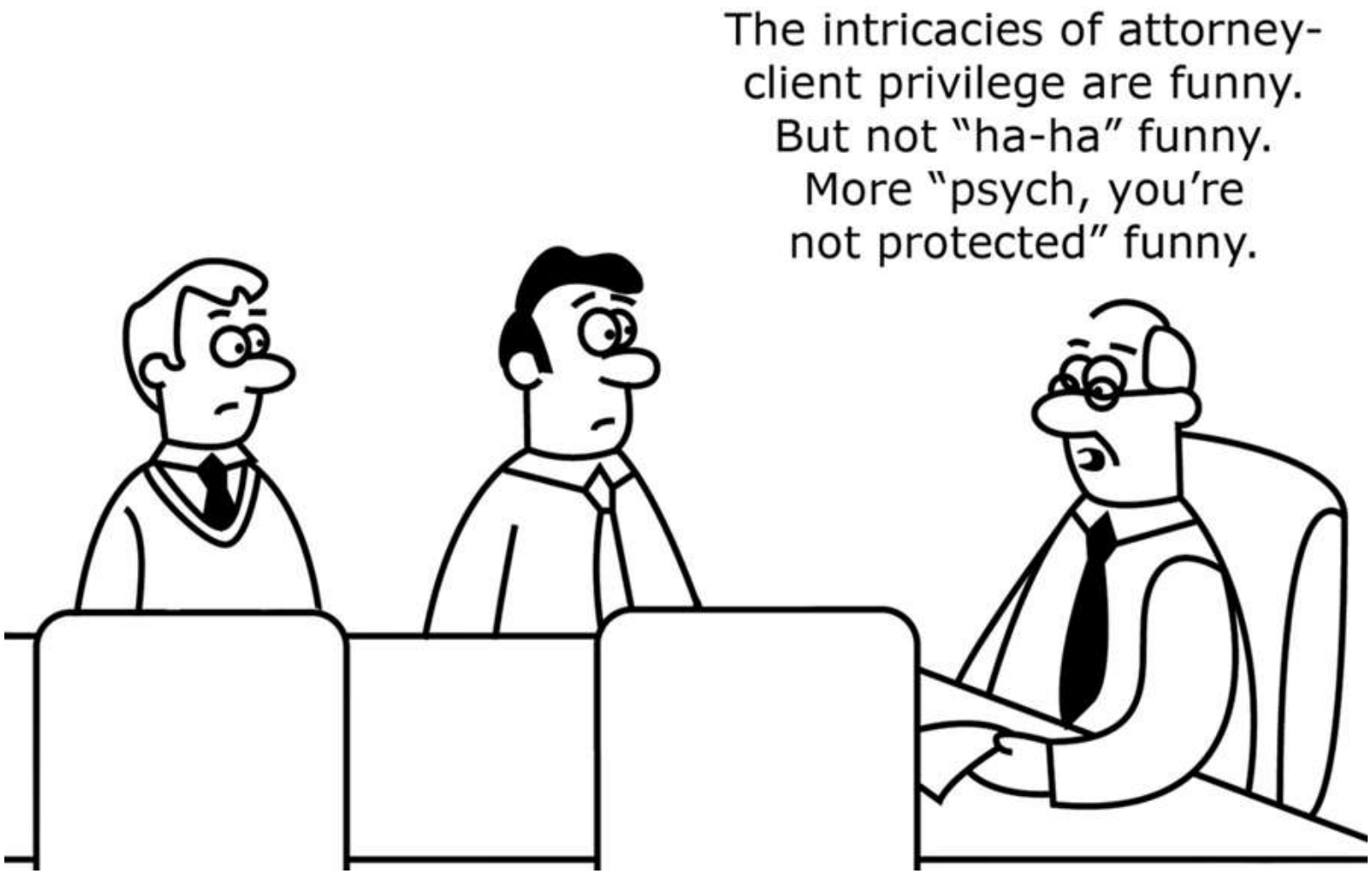
Attorney Client Privilege

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

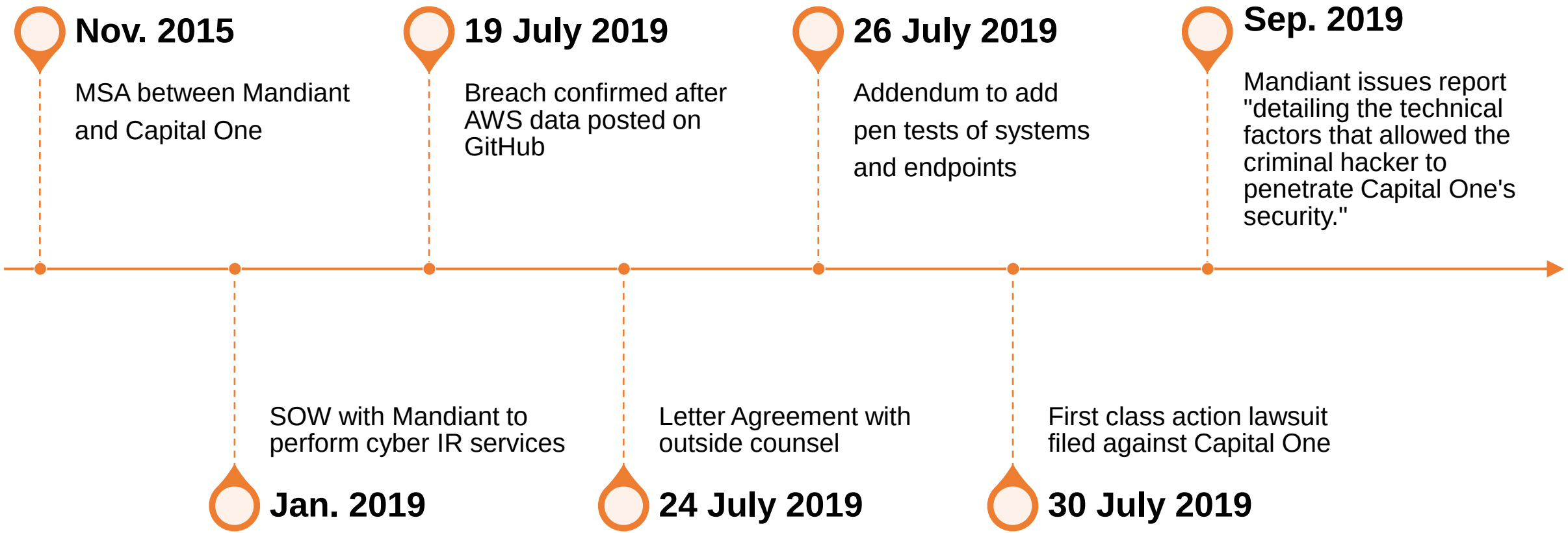
Work Product Doctrine

- 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.

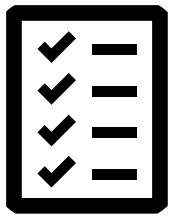
When Do The Protections Apply?



Case Study: *In Re: Capital One (2020)*

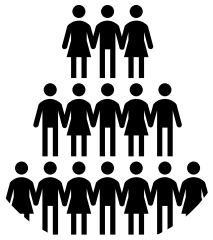


Capital One Reasoning



Scope of Work

Payment



Use and Disclosure

"There is no question that at the time Mandiant began its 'incident response services' in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach. Therefore, the determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation."

Case Study: *Wengui v. Clark Hill (2021)*

"…Clark Hill has not met its burden to show that the Report, or a substantially similar document, would [not] have been created in the ordinary course of business irrespective of litigation…The problem for the defense here is that its two-track story finds little support in the record…. Although Clark Hill papered the arrangement using its attorneys, that approach 'appears to [have been] designed to help shield material from disclosure' and is not sufficient in itself to provide work-product protection. "

Key Considerations

- Dual Track – No documents, report or findings from non-privileged "investigation"
- D&P referred to as "incident response team"
- Sharing of D&P report with IT and FBI
- Use of report for remediation and system hardening

Case Study: *In Re Rutter's Data Security Breach* (2021)

- May 2019: Rutter's received two Carbon Black Defense alerts identifying the execution of suspicious scripts and indications of potentially compromised credentials.
- Rutter's retained outside breach counsel "to advise Rutter's on any potential notification obligations."
- Counsel thereafter retained Kroll Cyber Security "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident."
- In the subsequent data breach litigation, plaintiffs sought both the forensics report produced by Kroll and "related communications" between Kroll and Rutter's.

Adverse Facts in Rutter's

The agreement between Rutter's and Kroll stated that the "purpose of the investigation was to determine whether data was compromised, and the scope of such compromise if it occurred."

→

The agreement also indicated that the vendor was merely retained to collect data, monitor IT equipment, and determine whether it had been compromised.

→

There was evidence that the report would have been prepared regardless of whether a suit was ultimately filed.

↓

There was no evidence that the law firm received the report before Rutter's did.

→

Holding: forensic report discoverable.

In-House Counsel Lessons

▪ **Retention**	Allow outside counsel to retain the forensics firm
▪ **Agreement**	Clearly define the legal advice sought and purpose in retainer agreement
▪ **Payment**	Pay for litigation-related cybersecurity services from your litigation or legal budget.
▪ **Different Forensic Investigators**	Outside counsel should be instructed not to use the same cybersecurity firm as the organization has formally retained to investigate/remediate cyber incident.
▪ **Limit Audience and Use**	Strictly limit the distribution of any post-breach forensic report to those with a litigation need-to-know.

EXTERNAL REPRESENTATIONS

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

FTC Enforcement

- FTC consistently goes after companies that do not accurately represent their data privacy and security practices.
- Case Study: *In Re Residual Pumpkin Entity* (2021)
- Representations:
  - email responses to commonly asked questions: “CafePress.com also pledges to use the best and most accepted methods and technologies to insure [sic] your personal information is safe and secure.”
  - Check out page: “Safe and Secure Shopping. Guaranteed.”
- Negotiated Settlement in March 2022:
  - $500,000 fine
  - Establish and implement comprehensive information security program.
  - Subject to third-party biennial assessments for the next *20 years*.

FTC Gearing Up

- FTC Chair Lina Khan's speech at IAPP Summit (April 2022).
- "[T]he realities of how firms surveil, categorize, and monetize user data in the modern economy invite us to consider how we might need to update our approach further yet."
- FTC is considering initiating rulemaking to address commercial surveillance and lax data security practices.
- Khan: the current "notice and consent" model is "outdated and insufficient," with the criticality of modern technology to everyday life limiting consumers' alternatives.
- TL; DR: Get ready for more FTC action on privacy matters.

California AG Enforcement

- CCPA Notice And Cure
- Office of the Attorney General (OAG) is responsible for enforcing the CCPA.
- OAG began sending notices of alleged noncompliance to companies on July 1, 2020, the first day CCPA enforcement began.
- Once a company is notified of alleged noncompliance, it has 30 days to cure that noncompliance.

California AG Enforcement, Companies Targeted

- **Industry: Social Media Platform**
- A business that launched a social media platform and advertised itself as being pro-privacy failed to inform consumers about their CCPA rights.
- The business also exchanged personal information about users' online activities with various third-party analytics providers but did not post the required notices or provide consumers with methods to opt-out of the sale personal information.
- After being notified of alleged noncompliance, the company updated its privacy policy and removed all third-party trackers from its app and website.

- **Industry: Children's Toys Distribution**
- A business that distributes children's toys did not provide notice of the required CCPA consumer rights, did not include the methods for consumers to exercise their CCPA rights to request to know and delete, did not list the categories of personal information it disclosed, and did not state whether or not it had sold personal information in the past 12 months.
- The business also claimed in its privacy policy that it could charge a fee for processing a consumer's request to know.
- After being notified of alleged noncompliance, the business updated its privacy policy to address these issues.

The Cornerstones: Accurate, Current, Reliable

What Information You Collect, How You Collect it, and What You Do With it.

Who You May Share Data With

Contact Information

Consumer Rights

Mandatory Disclosures (Cookies etc.)

Accurate

Privacy Policy “DON’Ts”

Privacy Policy

Effective Date: July 19, 2018

Mansueto Ventures LLC ("**Mansueto Ventures**" or "we") adopted this Privacy Policy to reflect our commitment to protecting your privacy. We take the collection of personal information from our Users seriously and are committed to protecting each User's privacy in accordance with this Privacy Policy.

In this Privacy Policy, we use the term "User" to include any individual who accesses and uses any of the Services,

Set it and forget it

- Annual update required
- Must reflect current practices

DON'T

What Information We Have & Where We Get It

We collect and store different types of information about you when you create an account, buy tickets, contact us, and use our websites, apps and social media.
Learn More

How We Use Your Information & Why

We collect and use your information for lots of reasons such as helping you get into the shows you love, sharing news, for marketing and as otherwise required by law.
Learn More

Who We Share Your Data With & Why

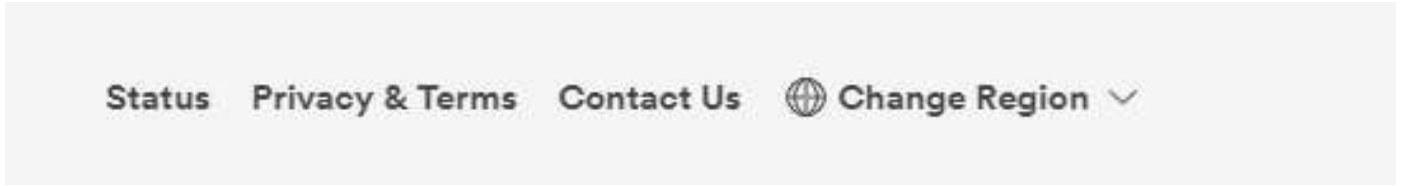
We may share your information with the event providers as well as other third parties associated with the service provided.
Learn More

Write in Legalese

- (aim for 6th grade)
- Transparency = Trust

ACC Association of Corporate Counsel SheppardMullin

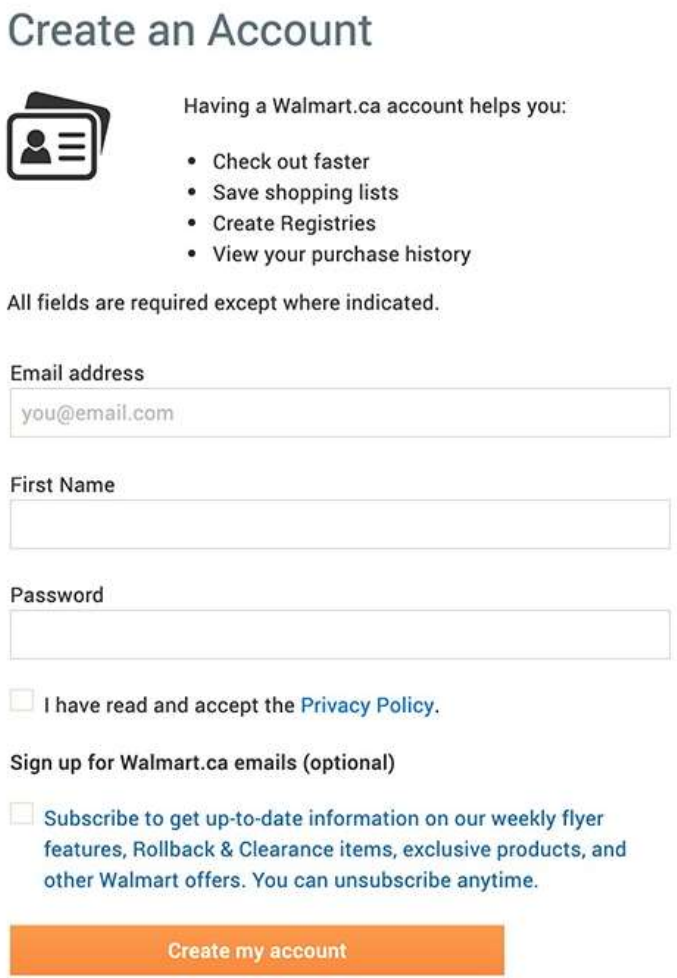
DON’T



Hide the Privacy Policy

- Accessible from any page
- Use the word “privacy”

DON'T



Forget to ask for consent

- Not enforceable in most jurisdictions

Security of your Personal Information

Title21Health.com strictly protects the security of your personal information and honors your choices for its intended use. We carefully protect your data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

Your personal information is never shared outside the company without your permission, except under conditions explained above. Inside the company, data is stored in password-controlled servers with limited access.

Make unnecessary promises

- Stick to the law
- Avoid use as a “weapon” following a data security incident

Questions?