

California Privacy and Social Media Concerns

ARMA San Diego

Wednesday, November 14, 2018

By: John Isaza, Esq., FAI

Course Objectives

- 1 Discuss concrete examples of areas where California privacy legislation and retention requirements may conflict;
- 2 Obtain best practices on ways these challenges can be addressed;
- 3 Discuss Social Media challenges and recent case law.

Part I

California Privacy vs. Retention

Focus of the CA Consumer Privacy Act (CaCPA)

Consumers rights with respect to their personal data:

"Data that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household."

An Info Security & Privacy Compliance Sea-Change

Background	Scope & Requirements	Comparison w/Other Laws
CA as a Privacy/Info Security Leader	Is your organization impacted?	State: MA, IL
Effective date	Key New Requirements	Federal: Various Agency Privacy Acts (e.g., FTC, FCC, DOJ, HHS)
What this Act does: <ul style="list-style-type: none">Grants unprecedented control to consumers over their personal information	Implications for your Organization	Global: GDPR



Legislation Conflicts



**Right to be forgotten
& retain no longer
than needed**

California Consumer
Privacy Act provisions

vs.



**HR records retention
requirements**

Data Lakes or Big Data
retention and monetization

Part II

Best Practices Solutions to Privacy vs.
Retention Tug of War



Best Practice Approaches

- ✓ Common sense approach to regulatory conflicts
- ✓ Anonymization and Pseudonymization
- ✓ Ask for agency guidance or opinions



**How do you
grapple with
the problem?**

- ✓ Identify privacy & disposition requirements – what must you destroy and how soon?
- ✓ Know your retention requirements – what must you keep and for how long?
- ✓ Make RRS your “first line of defense!”
- ✓ Identify content types with personal information
- ✓ Clearly document your decisions

Know your reg universe & data protection requirements

The screenshot displays the Virgo database interface for data protection requirements. The top navigation bar includes 'Citations', 'Content Types', 'Repositories', 'Support', and user options like 'Setup', 'Admin', 'My Account', and 'Sign Out'. A search bar on the left shows '7,145 Results' with a 'Filter' button. A 'Requirement Type' filter is applied, showing 'Disposition' with a count of 1. The main table lists various legal requirements from different jurisdictions.

Country	Requirement	Text	Requirement Type
Argentina	Law on Protection of Personal D...		Disposition
European Union	General Data Protection Regulati...		Disposition
European Union	General Data Protection Regulati...		Disposition
European Union	General Data Protection Regulati...	Where the controller has made the data public and must, pursuant to the above, er...	Disposition
Germany	Bundesdatenschutzgesetz (Fede...	Personal data may	Disposition
Germany	Pflanzenschutz-Geräteverordnun...	Personal data con	Disposition
Hungary	Act CXII of 2011 on Informational...	(1) Where a perso	Disposition
Lithuania	Law on Legal Protection of Pers...	Personal data mus	Disposition

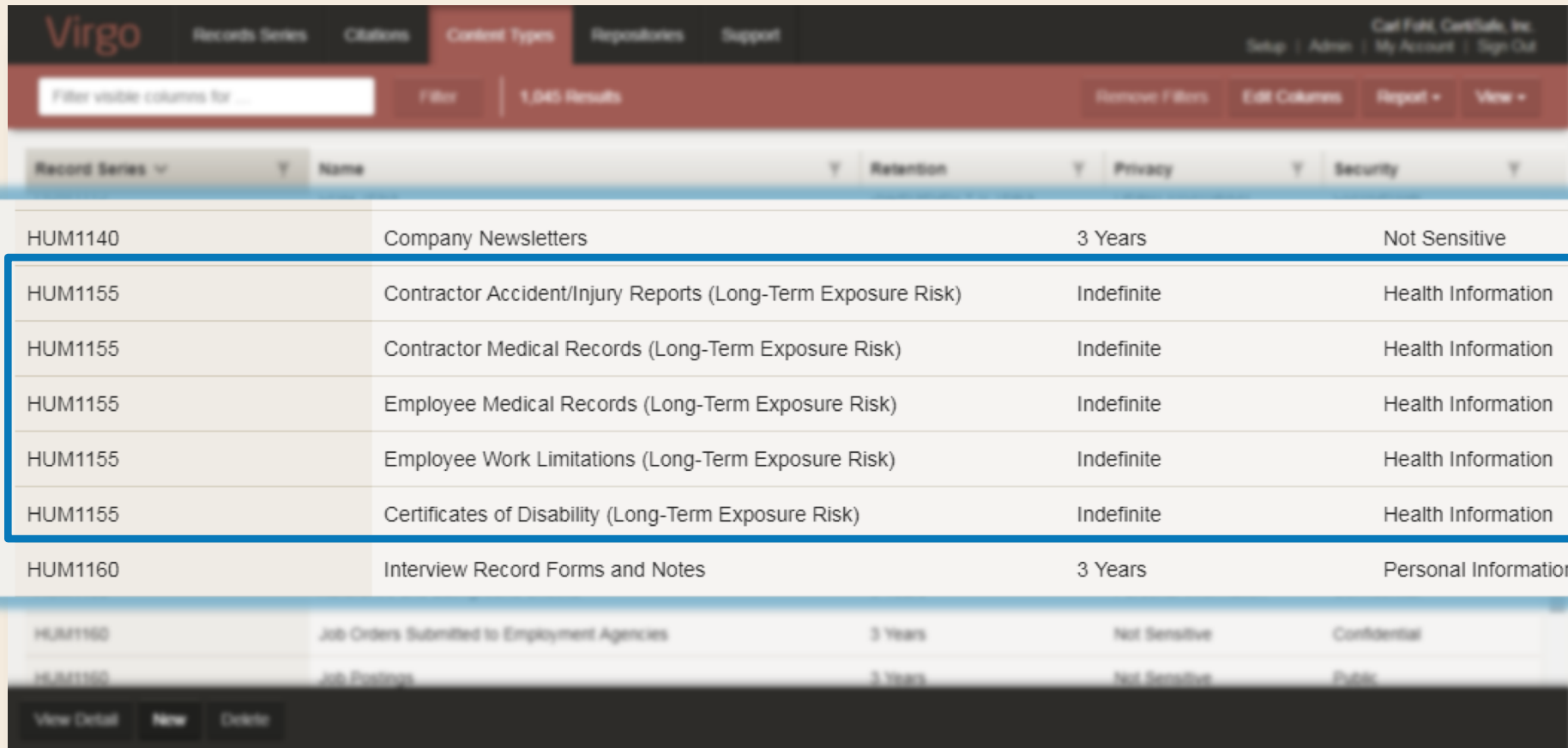
The bottom section shows the 'Virgo' logo and navigation tabs for 'Records Series', 'Citations', and 'Content Types'. A search bar contains the text 'data protection' with a 'Filter' button and '16 Results'.

Know Records with long legal retention periods...

The screenshot displays the 'Virgo' Records Series interface. On the left, a sidebar for record 'HUM1155' lists various fields like Code, Name, Description, Function, Departments, Status, Public Notes, Retention, Retention, Trigger Event, Exceptions, and Authority. The main panel is titled 'Mapped Citations' and shows a table of legal references. The table has columns for Jurisdiction, Citation, Retention, Considerations, and a 'Defining' checkbox. Three citations are listed: one from the United States (29 C.F.R. § 1910.1018(q)(2)(iv)), one from Italy (Testo unico in materia di sicurezza sul lavoro), and one from Malaysia (Occupational Safety & Health Regulations). Each citation has a 'Yes' button in the 'Defining' column. The interface also includes buttons for 'Map Citations', 'Unmap Citations', and a search bar for 'Filter mapped citations...'.

<input type="checkbox"/>	Jurisdiction	Citation	Retention	Considerations	Defining
<input type="checkbox"/>	United States	29 C.F.R. § 1910.1018(q)(2)(iv)	40 years, or for the duration of employment plus 20 years whichever is longer		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Italy	Testo unico in materia di sicurezza sul lavoro [Consolidated Law on Safety at Work] (Legislative Decree 81/2008), Art. 243	40 years after cessation of exposure to agents, carcinogens and mutagens		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Malaysia	Occupational Safety & Health (Use & Standards of Exposure of Chemicals Hazardous to Health) Regulations 2000, Reg. 13(a)	30 years		<input checked="" type="checkbox"/>

... which often contain personal data



The screenshot shows the Virgo Records Series interface. The top navigation bar includes links for Records Series, Citations, Content Types, Repositories, and Support. The user is logged in as Carl Foltz, Carlisle, Inc. The main content area displays a table of records with columns for Record Series, Name, Retention, Privacy, and Security. A blue box highlights a group of records containing health information.

Record Series	Name	Retention	Privacy	Security
HUM1140	Company Newsletters	3 Years	Not Sensitive	
HUM1155	Contractor Accident/Injury Reports (Long-Term Exposure Risk)	Indefinite	Health Information	
HUM1155	Contractor Medical Records (Long-Term Exposure Risk)	Indefinite	Health Information	
HUM1155	Employee Medical Records (Long-Term Exposure Risk)	Indefinite	Health Information	
HUM1155	Employee Work Limitations (Long-Term Exposure Risk)	Indefinite	Health Information	
HUM1155	Certificates of Disability (Long-Term Exposure Risk)	Indefinite	Health Information	
HUM1160	Interview Record Forms and Notes	3 Years	Personal Information	
HUM1160	Job Orders Submitted to Employment Agencies	3 Years	Not Sensitive	Confidential
HUM1160	Job Postings	3 Years	Not Sensitive	Public

At the bottom of the table, there are buttons for View Detail, New, and Delete.



Time for Risk-Based Analysis...

Document Your Decision



Private Comments ▾

Carl Fohl

Leave a new comment.

Comment

Carl Fohl

commented on Oct 29, 2018 10:13:47 AM

[Delete](#) | [Edit](#)

IG Steering Committee has decided to create a separate record series to cover health/medical records for EU employees. See HUM1155-EU for the EU-specific retention period.

Part III

Social Media Concerns

The Broad Standard of Discovery

Rule 26 (b) (1) Scope in General

Unless otherwise limited by court order, the scope of discovery is as follows:

- Parties may obtain discovery **regarding any nonprivileged matter that is relevant** to any party's claim or defense **and proportional to the needs of the case**, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit .
- Information within this scope of discovery **need not be admissible in evidence to be discoverable.**

(Emphasis added.)

Rule 37(e): Sanctions for Failure to Preserve ESI

If [ESI] that should have been preserved in the anticipation or conduct of litigation is lost because a **party failed to take reasonable steps to preserve it**, and it cannot be restored or replaced through additional discovery, the **court may**:

- Upon a finding of prejudice to another party from loss of the information, order measures no greater than necessary to **cure the prejudice**; or
- Only upon finding that the **party acted with the intent to deprive** another party of the information's use in the litigation:
 - **Presume** that the lost information was **unfavorable** to the party;
 - **Instruct the jury that it may or must presume** the information was unfavorable to the party; or
 - **Dismiss the action** or enter a default judgment.

(Emphasis added.)

Types of Discoverable Accounts

Defendants have requested:

- Every online profile
- Post, Message, Tweet, Reply, Retweet
- Status update, wall comment
- Groups joined, activity streams, blog entries
- Photograph and videos posted
- All online communications

Effect of Privacy Settings

Palma v. Metro PCS Wireless, Inc., 18 F.Supp.3d 1346 (M.D. Fla. 2014)

- Total amount of hours worked were at issue.
- Plaintiff activated a social media site's privacy settings to restrict who may access and view her postings.
- Court found that privacy settings do not provide blanket exemption from discovery.
- Plaintiff must honor her discovery obligations even if the requested discovery concerns private information.

Production of Log-In's and PW's

Moore v. Wayne Smith Trucking Inc., No. Civ. A. 14-1919, 2015 WL 6438913, at *2 (E.D. La. Oct. 22, 2015)

- Motorcycle accident case.
- Court declined to require Defendant to share his log-in or password information with Plaintiffs.
- Court directed that Defendant postings be made available to Defendant's counsel and that they be reviewed by Defendant's counsel—not Defendant himself—to determine whether they fit into one or more of the categories of discovery.

Types of Discoverable Accounts (cont'd)

Artt v. Orange Lake Country Club Realty, Inc., Case No. 6:14–cv–956–Orl–40, 2015 WL 4911086, at *2 (M.D. Fla. Aug. 17, 2015)

- Employment compensation of unpaid wages case.
- Defendants sought content on Facebook, MySpace, Instagram, LinkedIn or other social networking accounts posted at any time between 7:00 am and 7:00 pm on any date between June 19, 2011 and her last day of employment.
- Court found the request was overbroad, unduly burdensome, and unreasonable.

Attempts to Limit Based on Time Frame

Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 116 (E.D.N.Y. 2013)

- Disability discrimination case, with focus on emotional state of plaintiff.
- Defendants requested the Facebook archive for Plaintiff from 2006 (the year Facebook became available) until her death in 2013.
- Court found the scope of Defendants' request was flawed because it was not limited to a reasonable period of time.
- The court limited the scope. It allowed a sampling of Plaintiff's Facebook activity for the period November 2011 to November 2013, and limited to any "specific references to the emotional distress [Plaintiff] claims she suffered" in the Complaint, and any "treatment she received in connection [there]with."

Retention of Websites

McFadden v. Washington Metro. Trans., 168 F. Supp. 3d 100 (D.D.C. Mar. 7, 2016)

- Case of defamation and infliction of emotional distress
- Plaintiff proffered a screen shot of the defendant's web site, in which he represented that he does business "on behalf of attorneys, insurers, and employers in the state of Maryland and Washington, D.C. areas."
- By the time this matter was before the court, the web site had been taken down.
- Court granted further discovery into the issue of where defendant does business.
- Court noted that it was "troubling" that the web site no longer existed.
- Warned if defendant cannot produce a copy of what was posted prior to hearing, sanctions under the amended Rule 37(e) possible.

WhatsApp Messages

Moulton v. Bane, No. 14-cv-265, 2015 WL 7776892 (D.N.H. Dec. 2, 2015)

- The defendant in this action replaced his smart phone while the action was pending, and in the process lost approximately 1,600 WhatsApp messages, which he assumed would be transferred over to his new phone by the cellular service provider.
- The plaintiff moved for spoliation sanctions, including an adverse inference instruction.
- Court found loss occurred through the routine operation of an electronic information system; that there was no evidence of intent to destroy discoverable evidence; and, that the messages were later recovered.
- No evidence of intentional misconduct for serious sanctions.

General Cell Phone Activity

Restrepo v. Carrera, No. 3D15–1964, 2016 WL 231955 (Fla. Ct. App. 3d Dist. Jan. 20, 2016).

- Deadly accident case.
- The Court of Appeals quashed an order from the trial court requiring petitioner to provide information regarding all her cell phone activity during the six hours before the time of the crash and the six hours after the crash.
- Appeals Court found that the lower court order violated petitioner's Fifth Amendment rights.

Discovery of Emojis

- Emoticons = emotion + icon (portmanteau)
 - Kaomoji: `¯_ (ツ) _/¯`
- Emoji = “picture word” (Japanese)
 - Unicode emojis = standard definition but proprietary implementations



- Proprietary emojis (sometimes called “stickers”) = unlikely to work across platforms, so omitted or replaced with placeholder

Interpretation Issues (1)



Emojis are integral to a conversation

- Emojis can change the meaning of text ;-)



Emojis pose interpretative challenges

- No dictionary
- Dialects/cultural variations
- Unsettled grammar rules



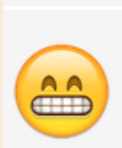
Conveying emotions

- What does “unamused” face mean?
- “disappointment,” “depressing,” “unimpressed” or “suspicious”

Interpretation Issues (2)



Technology mediation changes the sender's meaning



- Intra-Platform Version Incompatibilities
 - Cross-Platform Depiction Diversity
 - Cross-Platform Omissions
- Adjudicators may need to see exactly what *both* sender and recipient saw



Emojis as Evidence

- Emojis as courtroom evidence – 80+ cases published to date
- Displaying emojis in opinions
- Searchability

Final Points to Remember

1. Privacy settings do not mean information is not discoverable
2. Courts not inclined to grant unfettered access to accounts, especially passwords and user names
3. Discovery likely if provide very strict and narrow time frames that are relevant to issues at hand
4. Good practice to retain snap shots of website content, especially if anticipated litigation is looming

Questions?

John.Isaza@InfoGovSolutions.com

(949) 632-3860 Mobile

