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

<table>
<thead>
<tr>
<th>CA as a Privacy/Info Security Leader</th>
<th>Is your organization impacted?</th>
<th>State: MA, IL</th>
</tr>
</thead>
</table>

## Scope & Requirements

<table>
<thead>
<tr>
<th>Effective date</th>
<th>Key New Requirements</th>
<th>Federal: Various Agency Privacy Acts (e.g., FTC, FCC, DOJ, HHS)</th>
</tr>
</thead>
</table>

## Implications for your Organization

- Grants unprecedented control to consumers over their personal information

## Comparison w/Other Laws

- 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
Know Records with long legal retention periods…
… which often contain personal data

<table>
<thead>
<tr>
<th>Record Series</th>
<th>Name</th>
<th>Retention</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>HUM1140</td>
<td>Company Newsletters</td>
<td>3 Years</td>
<td>Not Sensitive</td>
<td></td>
</tr>
<tr>
<td>HUM1155</td>
<td>Contractor Accident/Injury Reports (Long-Term Exposure Risk)</td>
<td>Indefinite</td>
<td>Health Information</td>
<td></td>
</tr>
<tr>
<td>HUM1155</td>
<td>Contractor Medical Records (Long-Term Exposure Risk)</td>
<td>Indefinite</td>
<td>Health Information</td>
<td></td>
</tr>
<tr>
<td>HUM1155</td>
<td>Employee Medical Records (Long-Term Exposure Risk)</td>
<td>Indefinite</td>
<td>Health Information</td>
<td></td>
</tr>
<tr>
<td>HUM1155</td>
<td>Employee Work Limitations (Long-Term Exposure Risk)</td>
<td>Indefinite</td>
<td>Health Information</td>
<td></td>
</tr>
<tr>
<td>HUM1155</td>
<td>Certificates of Disability (Long-Term Exposure Risk)</td>
<td>Indefinite</td>
<td>Health Information</td>
<td></td>
</tr>
<tr>
<td>HUM1160</td>
<td>Interview Record Forms and Notes</td>
<td>3 Years</td>
<td>Personal Information</td>
<td></td>
</tr>
</tbody>
</table>
Time for Risk-Based Analysis…
Document Your Decision

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


- 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


• 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)


- 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


- 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.”
RetentionPolicy of Websites


• 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


• 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


• 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

www.AskVirgo.com
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

www.AskVirgo.com
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