Cooley

Information Retention Policies and E-Discovery

Best Practices & New Developments

Erin Trenda

Ruth Hauswirth

Matthew Krengel

SD ACC All Day MCLE September 22, 2021

Erin Trenda

Erin Trenda is a business litigator. Her practice focuses on contract disputes, trade secret matters and other intellectual property litigation, and commercial tort claims. Erin has experience litigating all stages of a case, from discovery and motion practice through trial, post-trial motions and appeal. She has been on several trial and arbitration teams that have successfully litigated disputes to a decision on the merits.

Erin Trenda
Partner, Business Litigation
+1 858 550 6147
etrenda@cooley.com

Ruth Hauswirth

Ruth Hauswirth is Special Counsel and Head of Litigation & E-Discovery in Cooley's Litigation Department. She specializes in and oversees Cooley's E-Discovery and Information Retention/Governance counseling practice. Ruth leads Cooley's litigation and eDiscovery services department and advises clients on enterprise information and record retention, disposition and governance. Ruth is also an adjunct faculty member at the University of San Diego School of Law teaching Electronic Discovery Law and from 1999-2000, Ruth served as the Assistant Dean for Law and Technology at Santa Clara University School of Law. Ruth is a frequent speaker on topics related to e-discovery, information governance and how technology is changing legal practice and legal education, as well as well-being, mindfulness and compassion in legal practice.

Ruth Hauswirth
Special Counsel, Director of Litigation & E-Discovery

+1 858 550 6108
rhauswirth@cooley.com

Matthew Krengel

Matt Krengel counsels clients on information and records retention and governance, including policy and program development and implementation. He helps clients at the organizational level navigate compliance with regulatory and legal requirements and develop comprehensive and tailored corporate governance plans related to enterprise data as well as designing other important governance policies, such as legal hold response plans, social media, BYOD, permissible use and data disposition.

Matthew Krengel
Director of Information Retention Counseling
+1 858 550 6485
mkrengel@cooley.com

What We Will Cover Today

- **Information Retention and Governance:** Avoid default of retaining unused information indefinitely, while improving procedures to meet any duty to preserve
- **Protecting Confidential Information:** Maintain the confidentiality of commercially sensitive business information
- **New Developments and Considerations:** Address increased use of collaboration apps and other trends with work from home

Information Retention and Governance

Cooley

No General Duty to Preserve

- Absent knowledge or notice that would trigger duty to preserve, a company generally has the **right to dispose** of its own property, including electronically stored information, hard copy documents or tangible things
- **No general duty to preserve information, unless:**
  - Voluntarily assumed by contract
  - Required by statute or regulation
  - Actual or reasonably foreseeable litigation or government investigation

Duty to Preserve for Litigation

- **Trigger:** A party must preserve **discoverable information** when litigation or a government investigation is **reasonably anticipated or foreseeable**, meaning it is threatened, pending, actually filed or contemplated against an individual or organization
- **Scope:** A party has a duty to undertake **reasonable steps** to preserve **discoverable information** (relevant to claims and defenses and proportional to needs of case) in its **possession, custody or control**
- **Approach:** Highly **fact dependent analysis** with no bright-line rules; **reasonableness** (not perfection) is the standard

When Ordinary Circumstances …

- "It is, of course, not wrongful for a manager to instruct his employees to comply with a **valid document retention policy under ordinary circumstances**."

  Arthur Andersen LLP v. U.S., 544 U.S. 696, 704 (2005)

- "It goes without saying that a party can only be **sanctioned** for destroying evidence if it had a **duty to preserve it**."

  Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003)

Become Circumstances Requiring a Hold

- "Once a party **reasonably anticipates** litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to **ensure the preservation** of relevant documents."

  Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)

- Balancing "shred day" caselaw with newer regulations and focus on privacy rights
  - Example of tension in IP litigation: *Glaukos Corp. v. Ivantis, Inc.* (C.D. Cal.)

Reasonably Foreseeable

- Duty to preserve when litigation becomes **reasonably foreseeable**
  - Objective standard
  - Totality of circumstances
    - Litigation need not be imminent
    - Litigation can be contingent on occurrence of other events
- Any document retention policy adopted by company in context of litigation strategy will not shield it from spoliation charges

Hold Requires Reasonable Steps Not Perfection

- Train legal team and designated IT personnel on standard
- Ensure protocol in place to institute reasonable steps to preserve as soon as legal hold issues
- Promptly issue, implement and update legal holds as-needed
- Exercise caution in determining appropriate time to withdraw legal hold after trial or settlement

Information Retention Counseling

- Create defensible information retention, management and deletion policies and protocols
- Identify, categorize and secure sensitive confidential information
- Reduce costs of litigation and discovery
- Improve compliance with privacy regulations and retention rules
- Increase visibility into organizational data
- Enhance organizational and employee productivity with efficient access to information (and deletion of redundant or outdated data)

Areas to Address

- Information handling and confidentiality protection policies, including access control
  - Onboarding employee policies and procedures
  - Departing employee policies and procedures
- Records retention policies and schedules
  - Email policies
  - Application / electronic message policies
  - BYOD and other device management
- Legal Hold policies and procedures
- Digital signature policies
- Data projects (mapping, classification, minimization)

It is a Balancing Act

- Manage policy in a way that balances not retaining everything with any obligations to preserve information
- Always some potential risk of unknown future litigation where data would help (or hurt) case, or avoid tactical spoliation claim
- Question of timing to end legal hold for closed matters
  - Settlement
  - End of regulatory investigation
  - Decision on the merits / appellate process

Getting Buy-In from Decisionmakers

- Real costs of not implementing a defensible policy
  - Cyber security threats / data breach risk
  - Inefficiencies for employees
  - Litigation
- Outside counsel can help convey urgency to decisionmakers
- No one size fits all solution; need to customize approach to each organization's business needs, risk tolerance (or focus) and other factors

How this Helps Protect Confidential Information

Cooley

Definition of a Trade Secret

- Federal definition under the **DTSA (18 U.S.C. § 1839(3))**

  (3) the term "trade secret" means **all forms and types** of financial, business, scientific, technical, economic, or engineering **information,** including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

  (A) the owner thereof has taken **reasonable measures to keep** such information **secret**; and

  (B) the information derives **independent economic value**, actual or potential, from **not being generally known** to, and ***not being readily ascertainable through proper means*** by, another person who can obtain economic value from the disclosure or use of the information;

- California definition under **CUTSA (CCP § 3426.1(d))** does not include language on if "readily ascertainable by proper means"

Defining Other Confidential Information

- Companies want to maintain confidential information that may not rise to level of trade secret as confidential
- What is confidential information?
  - Often broadly defined (which can cause enforcement issues)
  - Information is not generally known
  - Has commercial value or utility to company, or is otherwise subject to protection (*e.g.*, PII data)
- California makes it tougher to contractually protect confidential information post-employment

Protecting Confidential Information

- It is critical to identify and organize confidential information
  - Securely stored
  - Limit access to information (need to know basis)
  - Designation protocols
- Why?
  - Foster enforceable and practical contractual protections
  - Inform critical stages of employee on-boarding and off-boarding / training
  - Avoid unintended intermingling of data / facilitate remediation

Employee Hiring

- Interview candidate
  - Document candidate source
  - Understand scope of role at current and former employers
  - Consider interview NDA prohibiting candidate from disclosing any confidential information belonging to any current or former employers
- Analyze any confidentiality, noncompetition and/or nonsolicitation agreements with current and former employers
  - Definition of confidential information
  - Choice of law and forum selection clauses

Employee Agreements

- EA should include commitment to protect, not disclose and not use company's confidential information except to perform job
- Secure representations re third party information
  - Employee will not use or disclose any confidential information belonging to any third party, including any former employers
  - Employee has disclosed any confidentiality agreement, nonsolicitation agreement, and/or noncompetition agreement with any third party, including any former employers
  - Employment does not and will not breach any such agreement

Employee On-Boarding

- Interview and train new employees to avoid intermingling of data
  - Confirm no retention of information belonging to former employer
  - Ensure any BYOD devices were scrubbed
  - Policy re outside data: Sliding scale between prohibit entirely or require review before materials placed on system or brought into office
- Consider additional post-hiring protections for technical and sales hires
- Be prepared to respond accurately and in detail to any demand letters from former employers

Employee Off-Boarding

- Exit interview is critical
- Remind in writing of ongoing confidentiality obligation; potentially renew contractual commitment in connection with severance being paid
- Scrub BYOD or any company devices employee is being allowed to keep
- Remain mindful of any ongoing access levels with executive-level consulting or cooperation agreements
- Keep detailed tracking records if a manager is inheriting any data
- Coordinate with IT on continued preservation of any data under legal hold

Business Professions Code §16600

- BPC § 16600 voids any contract to the extent "anyone is **restrained from engaging** in a lawful profession, trade, or business of any kind"
  - Post-employment noncompetition agreements are unenforceable
  - Customer nonsolicitation provisions are generally unenforceable
  - Viability of employee nonsolicitation provisions under *Loral* remains in question after *AMN Healthcare, Inc. v. Aya Healthcare Services, Inc*, 28 Cal.App.5th 923 (2018)
- Trade secret exception within contractual limits

Enforceability of Post-Employment Confidentiality Obligations

- It was generally understood that employers could prevent former employee from using company's confidential information with new employer without running afoul of BPC § 16600
- Called into question by *Brown v. TGS Management Company, LLC*, 57 Cal.App.5th 303 (2020)
  - Arguably limited to unique facts (highly-specialized field and context for alleged breach)
  - But warrants scrutiny of definition of "confidential information" and how post-employment confidentiality obligations are being enforced

No Inevitable Disclosure Doctrine

- No doctrine of inevitable disclosure for trade secrets in California
- Reasoning is that the doctrine functions as an injunction in violation of BPC § 16600 because it "creates a **de facto covenant not to compete**" and "run[s] counter to the strong public policy in California favoring employee mobility."

Whyte et al. v. Schlage Lock Co., 101 Cal.App.4th 1443, 1462 (2002)

New Developments and Considerations

Cooley

Impact of Work from Home

- Trade secrets and contractually-defined confidential information require reasonable steps to protect information
- WFH has raised numerous issues on protecting data
  - Secure means to collaborate remotely / platform settings
  - Shadow IT issues
  - Re-entry of employees / proper disposal of data at home
- Legal industry is on cusp of grappling with big discovery disputes after WFH (with the Great Resignation exacerbating issues)

Collaboration Apps

- Increased use of apps that allow multiple users to create and share content
  - Messaging / Chat Applications
  - Videoconferencing Services (with messaging components)
  - Document Management Systems (with shared editing)
- Apps were already in use, but WFH increased number of users, frequency of use, and volume of data
  - Traditional project / content management
  - Company communications
  - Remote operations / evening work
  - Coordination with outside counsel or other partners

Traditional E-Discovery Challenges

- Traditional data collection is custodian-specific
  - Company devices
  - Company servers
  - Company premises
  - Personal devices
  - Personal premises
- Some level of uniformity between devices
- Industry standards and best practices

E-Discovery Challenges for Collaboration Apps

- Data for apps is often hosted by vendor and not on devices
- Less uniformity means forensic tools are struggling to keep up
- Fewer industry standards with (best) practices still evolving
- Increased data volume
- Dynamic content / message streams
- Third party data / shared ownership

Thoughtful Deployment of Apps

- Manage access and know what applications are being used on company devices (and what is permitted on BYOD)
- Understand license terms for all applications
- Training for IT and users to inform of policies and facilitate appropriate use
- Determine best settings for business needs
- Consider scope of deployment (and track if not enterprise-wide)
- Balance business retention needs and preservation obligations

Question of Cost and Functionality

- Can company properly administer the application?
- Weigh cost and functionality of different versions
- Slack example
  - Free version has very little admin controls
  - Standard and Plus have more admin controls, but still some exclusions on what can be exported
  - Enterprise grid allows formal collection and export

Litigation Hold Notices Must Include Apps

- Each time a new application is deployed, think about litigation hold process and how you will retain and preserve data on each application
- Litigation hold notices should list all applications and be updated when new applications are deployed
- Custodian interview process should include questions about custodian's usage habits on each application
- Critical for in-house to coordinate with outside counsel on this

Collection Issues for Messaging Apps

- Scope of collection
  - Direct messages
  - Public channels
  - Private channels
  - Multi-Party direct messages
  - Files and attachments
- Available data
  - Application plan
  - Deletion policy
  - Privacy policy

Collection Issues for Cloud Storage

- Certain cloud storage providers cap amount of data that can be exported at one time
- This may mean targeted exports are required
- Important that employees maintain organized folder structures to assist with targeted collection
- In litigation, consider addressing early with opposing counsel during FRCP 26(f) conference and/or in ESI protocol

Review Issues for Messaging Apps

- Messaging format fosters a looseness of communication style that is subject to misinterpretation
- Vendors are developing ways to take file and render in a contextual way, so that reader can better understand
  - Text messages
  - Emojis
  - GIFs
  - Videos

Predictions

- New round of precedent setting fights in the e-discovery space
- Upward trend in discovery costs will continue
- Earlier retention and increased engagement of forensic IT specialists in advising clients and outside counsel
- Renewed focus on ESI protocol and early meet and confers between counsel
- Continued presence of spoliation claims (some with merit, others as strategic tactic)

Questions?

Cooley