What is defensible deletion?

What does the law say?

How do we get started?

What if something goes wrong?

Conclusion
The obligatory disclaimer

- This presentation is informational in nature and may not be relied upon as legal advice.
- All views expressed by each panelist are their personal views and do not necessarily represent the views of their companies.
- Nothing said here may be used against the presenters, their companies or their clients, or else they did not say it, they were just joking, or you misunderstood.
What is **defensible** deletion?

**Keep**

Keeping records needed for
- Business
- Regulatory compliance
- Legal compliance

**Records Retention Policy**

The application of a records retention policy that allows companies to delete electronically stored information in a systematic and defensible way

**Discard**

Eliminating record R.O.T.
- Redundant
- Obsolete
- Trivial
Why get rid of R.O.T.

- Difficulty finding relevant documents
- Unnecessary storage costs
- Increased privacy risks
- Increased litigation costs
By the numbers

5% | Records retention

25% | Business value

1% | Legal hold

69% | No business, legal or regulatory value

Compliance, Governance and Oversight Counsel (CGOC) 2012 Summit
By the numbers (cont.)

- Percent of files once filed are never referred to again: **90***
- Hours per day spent searching for information: **2.5**
- Average number of emails a user sends/receives a year: **40k**
- Percent of references are to records less than 3 years old: **95***

---

*The High Cost of Not Finding Information - IDC  
https://www.armedia.com/blog/federated-search-the-importance-of-being-able-to-find-information/  
***How to design a legally defensible records retention plan - ARMA  
A real-world example

In a three-year study by the legal team of a major chemical company, it was discovered that 50% of documents had been kept beyond their retention dates, resulting in over $12 million in needless discovery costs.
Let’s be real

Records retention: These valuable documents should be stored for five years.

This job got so much easier when I realized that nobody ever asks for anything back.

Used with permission from Andrews McMeel Syndication
The duty to preserve is triggered when litigation is “reasonably anticipated” (or when there is a statutory obligation)

“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”

Federal Rules of Civil Procedure, Rule 37(e): Failure to Preserve Electronically Stored Information

If electronically stored information 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:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

   (A) presume that the lost information was unfavorable to the party
   (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
   (C) dismiss the action or enter a default judgment

Federal Rules of Civil Procedure, Rule 37(e): Failure to Preserve Electronically Stored Information

If electronically stored information 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:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

   (A) presume that the lost information was unfavorable to the party
   (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
   (C) dismiss the action or enter a default judgment

Federal Rules of Civil Procedure, Rule 37(e): Failure to Preserve Electronically Stored Information

If electronically stored information 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:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

   (A) presume that the lost information was unfavorable to the party
   (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
   (C) dismiss the action or enter a default judgment

Federal Rules of Civil Procedure, Rule 37(e): Failure to Preserve Electronically Stored Information

If electronically stored information 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:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

   (A) presume that the lost information was unfavorable to the party
   (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
   (C) dismiss the action or enter a default judgment
CLEANING OUT THE DATA CLOSET
WHEN AND HOW TO DEFENSIVELY DELETE DIGITAL RECORDS

FRCP 37(e) Flow Chart

Has ESI been “lost”?  

Y  
Should the “lost” ESI have been preserved?  

N  
Did party fail to take reasonable steps?  

Y  
Can the “lost” ESI be restored or replaced?  

Y  
Restore or replace the “lost” ESI and produce

N

STOP

1 Subject to proportionality considerations  

2 If the Court elects not to apply 37(e)(1)  

3 If the Court elects not to apply 37(e)(2)

Was a party prejudiced by the loss?  

The Court may: Order measures no greater than necessary to cure the prejudice.

Was there specific intent to deprive?  

The Court may:  
(A) Presume the information lost was unfavorable;  
(B) Issue mandatory or permissive adverse inference instruction; or  
(C) Enter dismissal or default.

Rule 37(e)(1)

Rule 37(e)(2)

Presented by  
DLA PIPER & ZAPPROVED

© Eric P. Mandel 2014-16  
Available under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0).
Document retention polices are okay

“‘Document retention policies’ which are created in part to keep information from getting into the hands of others … are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.”

Principle 6 of the Sedona Conference Commentary on Information Governance (2014) provides that:

“The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.”
...And the comment to Principle 6 further explains:

“It is a sound strategic objective of a corporate organization to dispose of information no longer required for compliance, legal hold purposes, or in the ordinary course of business. If there is no legal retention obligation, information should be disposed as soon as the cost and risk of retaining the information is outweighed by the likely business value of retaining the information.... Typically, the business value decreases and the cost and risk increase as information ages.”
Defending the process

Organizations should not be required to defend their disposition of any information that takes place before the duty to preserve arises.
For many companies that do business outside the US, the GDPR (and similar data privacy laws elsewhere) may require deletion of information. The GDPR provides that:

- Data should be kept only as long as needed for its original purpose
- Individuals have the “right to be forgotten”
- Individuals have the right to access their own data and
- Companies are liable for data breaches and must notify individuals
Know thyself

Level 1
The least developed organizations practice only ad hoc, inconsistently implemented processes which creates significant risk and cost.

Level 2 and 3
More mature organizations demonstrate some consistency in managing information. Level 2 is more manual and Level 3 is more automated. These are more silo’ed efforts than Level 4.

Level 4
The most mature IG programs take an enterprise view and effectively work across stakeholder groups through integrated processes, systems and communications.
The 9-step plan

1. Obtain buy-in
2. Enact records retention policy
3. Plan for legal holds
4. Prepare to delete
5. Identify and prioritize R.O.T.
6. Classify records
7. Validate the process
8. Pull the trigger
9. Document the process
Obtain buy-in

- Prepare your case
  - Cost, risk, efficiency gains
- Get a champion
- Bring in the key stakeholders
  - IT
  - Legal
  - HR
  - Business units
Enact records retention policy

- Define what constitutes a “record”
- List and categorize record types
- Set retention period for each record type
- Consider legal and regulatory requirements
  - SOX, GLBA, HIPAA, SEC Rule 17a-4, FRCP
- Document the policy
- Provide training on an ongoing basis
Records retention policy: best practices

- Simplify retention schedule
- Separate location for records
- Minimize human intervention
- Take a top-down approach
- Seek reasonableness
- Eliminate complicated triggers
- Rules must be absolute
- Resist permanent retention
- One schedule to rule them all

Plan for **legal holds**

It is defensible to delete information at the conclusion of litigation, pursuant to a company’s usual data retention policy. This includes data from all sources, such as outside counsel, experts, vendors, and opposing counsel and their experts and vendors. Remember that this is subject to any overlapping legal hold obligation.
Prepare to delete

Deletion must be:

- In good faith
- Neutral
- Systemic
- Universally applied
IDENTIFY AND PRIORITIZE R.O.T.

**Tools**
- Interview and questionnaires
- Legal hold systems
- Document management systems
- Email compliance centers
- Data maps
- Spreadsheets

**Sources**
- Hard copy
- Backup/disaster recovery
- Legacy systems
- Email archives/PSTs
- Old litigation collections
- File shares
- Cloud repositories
- Email

**Methods**
- Go forward
- Look back
### 3 approaches

There are 3 approaches to consider when cleaning out R.O.T.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go forward</td>
<td>Information governance program for retention or deletion of newly created data on a going-forward basis</td>
</tr>
<tr>
<td>Look back</td>
<td>Universal program to go back and clean out existing R.O.T</td>
</tr>
<tr>
<td>Start small</td>
<td>Starting small program to clean out types of unnecessary data (while using neutral policy), to show quick success.</td>
</tr>
</tbody>
</table>
Classify records

Low vs. medium vs. high hanging fruit

- Records prior to a certain cutoff date (e.g., more than 10 years old)
- Higher risk (archival, environmental, real estate, legal, pension) vs. lower risk (sales, routine operations) records
- Identify highest value/risk litigation holds
- Identify records with more detailed/reliable indexes and word searchable vs. those that are poorly indexed/not searchable
Validate the process

- Validate throughout the process
- Use statistical sampling to expedite review
- Confirm results with subject matter experts
- Document the results
Pull the trigger

- Once records are cleared for disposal, choose a disposal method that will protect the information from reconstruction.
- If using electronic means to delete from a larger universe, test with copies before applying to originals.
- Once ready to apply to live data, start with a sample to identify any remaining issues.
Document the process

- Keep written records to support the identification and disposal process, including any statistical analyses performed.
- Get litigation counsel signoff before deleting any records originally subject to legal holds.
- Consider obtaining opinions of counsel on other remediation steps.
Defensible deletion: best practices

- Take a cross-functional approach
- Get executive sponsorship
- Start small, show results
- Keep it evergreen
Avoid common pitfalls

Some of the more common pitfalls that organizations run into when trying to implement defensible deletion include:

- Overreliance on humans
- Lack of training
- Lack of buy-in
- Taking on too much
- Forgetting about legal holds
- Analysis paralysis
What if something goes wrong?

What if you later discover you deleted data needed for business or eDiscovery purposes?

• You will be protected by 37(e) if you acted in good faith

• Check if the data is available from an alternative source
In conclusion

• Be aware of when to implement a legal hold

• However, document retention policies are completely permissible

• In fact, deletion of information is necessary in some instances
Q&A