Defensible deletion: The proof is in the planning

eDiscovery Alert

5 February 2021

By: Andrew J. Peck | Jennifer M. Feldman | Leeanne Sara Mancari | Dennis Kiker

Most companies maintain vast amounts of unneeded data and can decrease legal and compliance risk and minimize financial burden if they retain less ROT (redundant, obsolete and trivial data). Unfortunately, eliminating ROT, often referred to as “defensible deletion,” can seem challenging. Here, we provide a framework for making defensible deletion an attainable goal. The key lies in planning.

What is defensible deletion?

Prospectively, defensible deletion involves the ongoing and routine elimination of unneeded data, in real time or pursuant to a prescribed schedule to avoid accumulation of ROT. Retroactively, defensible deletion involves identification and deletion of previously accumulated ROT. In either case, the “defensible” part of the proposition involves minimizing legal risk, particularly associated with spoliation of evidence.

Deletion can be … defensible

The first challenge most legal departments face is the question of whether any data can safely be deleted. The short answer is, “yes.” Companies are entitled to dispose of information they no longer need, so long as they do not violate regulatory requirements or litigation preservation obligations. As validated by the US Supreme Court, “‘Document retention policies,’ which are created in part to keep certain information from getting into the hands of others, including the

Government, are common in business. It is, of course, not wrongful for a manager to instruct employees to comply with a valid document retention policy under ordinary circumstances." *Arthur Andersen v United States*, 544 U.S. 696, 704 (2005).

"Best practice" dictates not only that a record *may* be destroyed when no longer required for any business, legal or regulatory purpose – it *should* be destroyed due to the many risks associated with over-preservation. The Sedona Conference, *Commentary on Defensible Disposition, Second Ed.*, 20 Sedona Conf. J. 179, 187, 199 (2019). These risks include unnecessary storage costs; compliance risks associated with retention of data subject to privacy regulations; compliance with contractual provisions concerning retention and disposition of confidential and other business information; reduced productivity due to difficulty in finding information; increased litigation risk; greater expense associated with discovery in future matters; and increased cyber-security risks. Id. at 199-214.

Lay a foundation for defensibility

Stakeholders should decide to dispose of information based on legal and business judgment, relying on sound processes and procedures, including:

1. **Records retention policy and schedule:** Ideally, companies document retention requirements in a policy and schedule, which lends certainty to decisions about what data are eligible for deletion. In the absence of a previously established policy, one can be developed for a targeted category of data as part of the defensible deletion initiative.
2. **Inventory of legal preservation obligations:** Most companies have legal holds in place, requiring preservation of certain data. Understanding the data categories subject to legal hold, and where that data resides, will allow stakeholders to more efficiently effectuate a defensible deletion project.
3. **Buy-in and support:** Any effort to dispose of data is likely to face opposition without executive support. The key is identifying the "win" for each affected constituent: reduced cost for the CFO, increased storage capacity and decreased complexity for the CIO, faster system performance and response times for the COO, etc. Eliminating ROT benefits every aspect of the business; it is simply a matter of identifying the benefit for stakeholders.

Understand the scope

Next, the stakeholders must understand and define the scope of the disposition initiative, which can be defined in many ways:

1. **Key driving forces:** Often, circumstances will make the scope clear. For example, retirement or upgrade of a system or migration to a new platform creates a unique opportunity to delete ROT from those sources. Similarly, release of a legal hold creates an opportunity for defensible deletion for data that was subject to the hold. Organizational transformations like a merger or acquisition create opportunities to identify and dispose of unneeded information as systems and data sources are integrated and consolidated.
2. **Departmental focus:** Individual departments can be the focus of a defensible deletion project. Reorganizations, relocations, or other circumstances may make a department open to a "house-cleaning" exercise for its own data.
3. **Enterprise-wide information governance:** Many companies are beginning to prioritize enterprise-wide information governance. Such efforts are ideal opportunities to launch a defensible deletion project, as they offer an early, demonstrable return on investment. If undertaking an enterprise-wide initiative, it is advisable to divide it into smaller projects, because it can be daunting to assess ROT on a company-wide level all at once.

Staff the project

Defensible deletion is a multi-disciplinary exercise requiring the knowledge and expertise of different members of an organization:

- Legal and compliance – to ensure compliance with legal and regulatory preservation obligations
- Business representative(s) for the functions responsible for the data – to understand which information has business value
- IT – a technical resource for execution
- Records management professionals – to advise on statutory retention requirements and prospective strategies
- Outside resources – depending on scope, complexity, and internal resource availability, there may be a need for outside resources to augment the above roles
- C-suite sponsors – to show support

Timing is everything

Timing is critical in two ways. First, to manage expectations. Data cannot be deleted instantaneously, particularly in large volumes. Actual execution will take time, the overall process will be iterative, and stakeholders must be cognizant of this.

Second, preservation obligations can arise unpredictably. Because the defensible deletion process takes time, it is necessary to plan for a “quiet” period during which new preservation obligations are unlikely to arise. Having a plan in place will enable the company to act quickly when a quiet period arises.

Data categorization

The key to success for a defensible deletion project is to focus on feasibility and not take on too much at once. Early wins with low-hanging fruit will demonstrate the value of the effort.

Once you understand the scope of data to be analyzed for potential disposition, it is time for the hard part, and the heart of the project – categorizing the data for deletion based on criteria allowing the stakeholders to assess the applicable retention schedules, legal preservation obligations, and business value.

Start by categorizing the data into three buckets (easy, medium, and hard) based on objective, identifiable criteria that enables differentiating data. Culling should be iterative, beginning with specific criteria such as, but not limited to, retention guidelines, date ranges, data type, custodian, department, applicability to legal hold, or accessibility. If circumstances warrant, subsequent culling efforts can be more targeted and refined, using search terms or other criteria. You can get creative. Relying on the advice of others experienced with these projects can be beneficial.

The three-bucket approach:

- **Easy.** This data is low-hanging fruit. It is readily identifiable and easy to understand whether it has any basis for retention.
  - Example*: The company may understand that it has no regulatory or legal obligations to keep data more than 10 years old. Accordingly, any in-scope data 10 years or older only needs to be assessed for business value.
- **Medium.** This data will require deeper analysis as to its content and retention obligations. It may be mixed data and not as easily recognizable.
  - Example*: The company may have a “data closet” of hard drives containing email data for a large legal hold that has now terminated. Retention requirements for that data has expired; however, various custodians have been placed on subsequent legal holds. In this situation, it is imperative to identify the data for each custodian subject to subsequent legal holds.
- **Hard.** This data will be the most complex to analyze. It may be completely unidentifiable or hard to access. It will be important to assess reasonableness and proportionality here.
  - Example*: The company has identified backup media it is no longer using and has not used for several years. The company can no longer access the backup without retaining an expensive vendor to analyze the media. The company believes that all information needed for regulatory purposes has been separately retained but is worried that data subject to legal hold may be on the backup. Here, because of reasonableness and proportionality, it may be more appropriate to assess whether any data is missing from the legal holds that may require preservation of backup media (than to assess what is on the backup media) and proceed accordingly.

*These examples are illustrative only and are not legal advice.

Document everything

A critical component of defensibility is documentation. Document the overall approach, the scope, the data classification process, and final execution.

Pull the trigger

The best approach to execution of the defensible deletion task is an iterative one, as depicted in the accompanying illustration.

1. **Data deletion:** This seemingly simple step can be surprisingly complex, as there is more than one way to delete data. The method will depend on the desired level of certainty. It is best to consult an IT professional who can outline the different standards of data deletion available.
2. **Validation:** However data are deleted, it is important to validate the results through sampling and testing.
3. **Further culling:** In many cases, one round of culling will achieve the desired objective; however, it is possible to continue culling using more advanced and refined data identification methods.

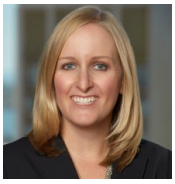
What if something goes wrong?

If the process has been well-planned, executed, and documented, the risk of sanctions for inadvertent spoliation of evidence is slight. Sanctions under Fed. R. Civ. P. 37(e) are available only when data "should have been preserved in the anticipation or conduct of litigation" and you "failed to take reasonable steps to preserve it." Planning a sound process and documenting its execution will generally demonstrate reasonableness and good faith.

Learn more about the legal aspects of defensible deletion by contacting the authors or any member of DLA Piper's eDiscovery and Information Management practice.

AUTHORS

Andrew J. Peck
Senior Counsel
New York | T: +1 212 335 4500
andrew.peck@dlapiper.com



Jennifer M. Feldman
Of Counsel
San Diego (Downtown) | T: +1 619 699 2700
jennifer.feldman@dlapiper.com

Leeanne Sara Mancari
Of Counsel
Los Angeles (Century City) | T: +1 310 595 3000
New York | T: +1 212 335 4500
leeanne.mancari@dlapiper.com

Dennis Kiker
Senior Attorney
Phoenix | T: +1 480 606 5100

dennis.kiker@dlapiper.com