

Reproduced with permission from Digital Discovery & e-Evidence, 15 DDEE 16, 01/08/2015. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

INFORMATION GOVERNANCE

The authors examine how organizations can lower preservation costs, risks and inefficiencies without increasing their exposure to judicial or regulatory sanctions.

Legal Considerations for Defensible Deletion Practices



BY JAMES FITZGERALD AND RICH VESTUTO

A common refrain from IT is that “storage is cheap,” which is true if just the costs of media are considered. However, this relaxed attitude towards a key component of information governance ignores the very real collateral costs of hoarding data.

For organizations subject to frequent litigation, regulatory requests or compliance audits, the untended, growing volumes of electronically stored information (ESI) held in data repositories significantly raises the costs and risks of eDiscovery. Proactively deleting unnecessary or irrelevant ESI helps contain or reduce the significant collateral costs of the common “keep everything” approach.

Staggering Statistics. In February 2014, Professor William H.J. Hubbard, assistant professor at the University of Chicago Law School, published a *Preservation Costs Survey*¹ that examined how organizations address preservation obligations and at what cost. Hubbard collected responses from 128 organizations ranging in size and industry. Some of the key findings from the larger organizations surveyed included the following:

¹ Preservation Costs Survey by William H.J. Hubbard, J.D., Ph.D., Assistant Professor of Law, University of Chicago Law School; February 18, 2014.

- Estimated preservation costs exceeded \$40 million per company per year;
- Slightly less than half of all preserved data is, at some point, collected, processed and reviewed; and
- Lowering time spent on legal holds by just 3 percent would save more than \$1 million per year.

Applying Defensible Deletion Practices

At its heart, defensible deletion is a process requiring adherence to clear business controls. Implementing a defensible deletion strategy requires a multi-faceted methodology that must be approached with a mind-set that recognizes “Rome wasn’t built in a day.”

The process should be ongoing, and organizations must be persistent in creating a strategy that is consistent, comprehensive and effective.

Key Considerations

1. Create information retention and disposition policies with executive buy-in.

■ Organizational buy-in. Effective information retention policies starts by having the right people at the table—representatives from IT, legal, records and information management and the respective business units.

■ Retention policy considerations. When drafting retention policies, the representatives must take into account what data must be retained, for what period of time, its strategic value to the organization and whether it is subject to a legal hold or compliance request.

Additional considerations should include multinational aspects, such as whether ESI is subject to the Foreign Corrupt Practices Act or to privacy requirements.

Social business content, like websites or third-party collaboration platforms, often must be part of the picture as well. Highly regulated organizations can expect growing regulations in this latter area.

■ Policy communication and enforcement. This is the area where most retention failures occur. The key to communicating and enforcing retention and disposition policies is simplicity—no one is going to read and then take action on a 200 to 300 page policy.

The policies should be easily understandable by outside parties (like judges) and should be included as part of the overall information governance plan with executive sponsorship.

Beyond communication, it is critical to deploy technology to monitor and enforce the policies, such as periodic repository sweeps for potential record declarations, as well as eliminating trivial and outdated information.

An up-to-date picture of what must be preserved, why and for how long enables organizations to move away from the “save everything” mentality.

2. Develop a consistent preservation hold process.

The principle challenge with managing the preservation process is that as more custodians and data stewards are added, the efforts to administer holds multiply. Maintaining an authoritative record of holds across all personnel and systems even when business requirements are dynamic requires structure and automation.

The following four steps are critical to preserving the right ESI while letting the disposition stage for irrelevant data proceed:

■ Establish an authoritative legal hold system. Legal and compliance operations, including defensible disposition processes, require a single version of the truth—a system of record about holds.

An authoritative hold system correlates all preservation activities associated with a matter, making it easy to audit and report on all data impacted by a case. It is this up-to-date picture of what must be preserved, why and for how long that enables organizations to move away from the “save everything” mentality.

■ Link to existing data infrastructure. Linking the legal hold system to the existing enterprise infrastructure, such as HR, asset and matter management systems and archives and records systems, gives the hold administrator access to the most current information about the people and repositories involved with holds and ensures ESI does not get accidentally deleted.

The risk of ESI spoliation is highest when custodians leave the organization.

Linkage to archives and records systems can also prevent “stranded holds” on data that can be safely deleted, which often happens when data stewards aren’t automatically notified that a case has concluded.

■ Control disposition of irrelevant ESI. A good disposition process has close ties with the authoritative hold system. When making sweeps through repositories to purge old files, the disposition process must ensure it has up-to-date information on which individuals and repositories are subject to holds for compliance or legal reasons.

ESI that is not deemed relevant to a legal hold or compliance request order should be moved to a temporary holding pen for final deletion. The “quarantine” period for this ESI is typically 30 to 90 days, and can serve as a backstop in the event an automatic deletion call is premature.

■ Document and follow the process. Documentation is arguably the most important part of the disposition process. If counsel cannot prove that the organization had a clear, well-designed process and that it was consistently followed, then its defensibility can be severely undermined. Organizations need to maintain a deletion log with triggering event details.

Courts are looking for a reasonable process; not a perfect one. Detailed documentation of the disposition process goes a long way to demonstrating reasonableness.

Conclusion

The unchecked growth of enterprise data has become especially burdensome for corporate legal, records management and IT teams. They are saddled with the Herculean task of preserving all potentially relevant ESI from an aging pile of ill-governed data amassed on cheap storage and then sifting through it in order to meet document production obligations during civil litigation and regulatory agency requests. Simply adding more storage capability does not solve the problem; it exacerbates it.

Defensible deletion addresses this problem by creating an orderly, repeatable process for eliminating ESI that has little or no business value and the potential of costly review by outside counsel.

Combining a comprehensive records retention policy with an authoritative legal hold system ensures that the disposition of old and irrelevant ESI can proceed in a defensible fashion. It allows organizations to meet discovery obligations while minimizing both document review and storage costs.

James FitzGerald, Sr. Director, Information Governance, drives the growth and positioning of Exterro’s eDiscovery and information governance solutions. He brings to Exterro more than 20 years of experience in strategic management for industry-leading complex software solution providers. Previously, he was Director of Product Management and Strategy for IBM for 10 years.

Rich Vestuto, Director, Deloitte Discovery and Dispute Services, specializes in providing legal insight, guidance and other technology-based data retention strategies to Deloitte’s corporate and law-firm clients. He has developed eDiscovery response plans, litigation hold policies, information governance strategies, defensible disposition tactics, early case assessment strategies and preservation/data acquisition plans, consulting in more than 200 litigations and investigations.